IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received September 9, 2021, accepted September 15, 2021. Date of publication xxxx 00, 0000, date of current version xxxx 00, 0000.

Digital Object Identifier 10.1109/ACCESS.2021.3113649

Blockchain and Autonomous Vehicles: Recent Advances and Future Directions

SAURABH JAIN[1], NEELU JYOTHI AHUJA[1], P. SRIKANTH[1], KISHOR VINAYAK BHADANE[2], BHARATHRAM NAGAIAH[3], ADARSH KUMAR[1], AND CHARALAMBOS KONSTANTINOU[4], (Senior Member, IEEE)

[1]School of Computer Sciences, University of Petroleum and Energy Studies, Dehradun 248007, India
[2]Amrutvahini College of Engineering, Sangamner, Maharashtra 422608, India
[3]Intralox, Breinigsville, PA 18031, USA
[4]Computer, Electrical and Mathematical Sciences and Engineering (CEMSE) Division, King Abdullah University of Science and Technology (KAUST), Thuwal 23955-6900, Saudi Arabia

Corresponding author: Adarsh Kumar (adarsh.kumar@ddn.upes.ac.in)

ABSTRACT Blockchain is an underlying technology for securing many real-time applications and their data. The automobile is one such sector in which auto-manufacturers are looking forward to accepting the advantages of distributed ledger technology in autonomous vehicles or systems and improving their products, customer satisfaction, and other valuable experiences. This work aims to find the significance of blockchain technology in Autonomous Vehicles, including Autonomous Electric Vehicles (AEV), Autonomous Underwater Vehicles (AUV), Autonomous Guided Vehicles (AGV), Autonomous Aerial Vehicles (AAeV), and Autonomous Driving. In this work, a comparative analysis of blockchain-integrated autonomous vehicle systems is explored to identify the present scenario and futuristic challenges. In addition to blockchain technology, the uses and importance of sensors, architectures and infrastructure requirements, vehicle types, driving modes, vehicles target and tracking approaches, intelligent contracts, intelligent data handling, and industry-specific use cases are also explored. This study is based on the exploration of recent technologies and practices. As autonomous vehicles are expected to be the future of intelligent transportation, this paper surveys recent advances in autonomous vehicles and systems and how blockchain can help in improving user experiences and improving industry practices. Finally, limitations of work, future research directions, and challenges associated with different autonomous vehicles and systems are presented.

INDEX TERMS Autonomous driving, autonomous systems, autonomous vehicles, autonomous underwater vehicles, autonomous electric vehicles, autonomous guided vehicles, blockchain, cryptocurrency, smart contract.

ACRONYMS

Acronym	Description
AAeV	Autonomous Aerial Vehicle
ACC	Adaptive Cruise Control
AEV	Autonomous Electric Vehicles
AGV	Autonomous Guided Vehicle
AIM	Autonomous Intersection Management
AI	Artificial Intelligence
AMR	Autonomous Mobile Robots
AQLPR	Adaptive Quasi-Linear Parity Relations
AS	Autonomous Systems
AiS	Air Sensors
AV	Autonomous Vehicles
BOEV	Battery Operated Electric Vehicle
BV	Bimodal Vehicle
CapEx	Capital Expenditure
CESS	Chemical Energy Storage System
CM	Corrective Maintenance
CMMSE	Cluster-based Minimum Mean Square Estimation
CVaaS	Connected Vehicles as a Service
DA	Driver Agent
DAV	Decentralized Autonomous Vehicle
DBFT	Delegated Byzantine Fault Tolerance
DL	Deep Learning
DMMSD	Dynamic Model-based Mean State Detection
DSRC	Dedicated Short Range Communication
DR	Demand Response
EESS	Electrical Energy Storage System

The associate editor coordinating the review of this manuscript and approving it for publication was Cong Pu.

ESS	Energy Storage Systems
EV	Electric Vehicles
ECESS	Electrochemical Energy Storage System
FAA	Federal Aviation Administration
FC	Fuel Cell
FCEV	Fuel Cell Electric Vehicle
FL	Federated Learning
GDP	Gross Development Product
GLRT	Generalized Likelihood Ratio Test
GPS	Global Positioning System
GS	Ground Sensors
GSM	Ground Sensor Modules
HALE	High Altitude and Long Endurance
HEV	Hybrid Electric Vehicle
IC	Internal Combustion
IDEA	Infeasibility Driven Evolutionary Algorithm
IMA	Intersection Manager Agent
IMU	Inertial Measure Unit
IV	Intelligent Vehicle
IIoT	Industrial Internet of Things
IoUT	Internet of Underwater Things
IoT	Internet of Things
IoV	Internet of Vehicles
KBPP	Knowledge-Based Path Planner
LALE	Low Altitude, Long Endurance
LASE	Low Altitude Short Endurance
LiDAR	Light Detecting And Ranging
LMS	Least Median Squares
LSN	Linear Sensor Networks
LTE	Long Term Evolution
LTE-A	Advanced Long-Term Evolution
JAMSTEC	Japan Agency for Marine-Earth Science Technology
MALE	Medium Altitude and Long Endurance
MAV	Micro UAeV
MCS	Mission Control System
MBARI	Monterey Bay Aquarium Research Institute
MEC	Mobile Edge Computing
MESS	Mechanical Energy Storage System
MUAeV	Mini UAeV
ML	Machine Learning
MMAE	Minimum Mean Absolute Error
MMSE	Minimum Mean Square Error
MRED	Mean Residual Error Detection
MNDC	Malicious Node Detection Algorithms
M-AIM	Multi-Agent AIM
NAV	Nano UAeV
NCC	Network Control Centre
NSGA-II	Non-dominated Sorting Genetic Algorithm-II
NSTL	Naval Science and Technology Laboratory
P2P	Peer-to-Peer
PoS	Proof of Space
PCs	Personnel Computers
PIHEV	Plug-in Hybrid Electric Vehicle
PID	Proportional Integral Derivative
PM	Preventive Maintenance
PeRL	Perceptual Robotics Laboratory
PHEV	P2P hybrid EVs
PoC	Proof of Concept
PoD	Proof of Driving
PoE	Proof of Event
PoW	Proof of Work
PoR	Proof of Reputation
RADAR	Radio Detection and Ranging
RAUVI	Reconfigurable AUV for Intervention Missions
REEV	Range Extended Electric Vehicles
ROV	Remotely Operated Vehicle
SAE	Society of Automotive Engineers
SDBCA	Sensor Data Bus Based Control Architecture
SNs	Sensor Nodes
SLAM	Simultaneous Localization And Mapping
SVM	support vector machine
TUAeV	Tactical UAeV
UAV	Underwater Autonomous Vehicle
UAeV	Unmanned Aerial Vehicle
UUAV	Unmanned Underwater Autonomous Vehicle
UUnV	Unmanned Untethered Vehicle
V2V	Vehicle to Vehicle
V2I	Vehicle to Infrastructure
V2X	Vehicle to Everything
V2SD	Vehicles to Smart Devices
V2HT	Vehicles to Home Technology
VTOL	Vertical Take-off and Landing
WLAN	Wireless Local Area Network
ZEV	Zero-Emissions Vehicle
ZKRP	Zero-Knowledge Range Proof

I. INTRODUCTION

AVs are widely discussed over the past few years in both academic and industry works. AVs are expected to be integrated with our lifestyle in either one or more forms, such as autonomous drone delivery systems, driverless cars, automated guided vehicles in warehouses, autonomous devices for home assistants, and AEV for green energy solutions. Autonomous vehicle, its type, usage, and application depends upon the level of automation. The story of autonomation in these vehicles has improved recently because of advancements and feasibility to integrate advanced technologies (like blockchain, industry 4.0, AI, ML, FL, ML, neural networks, cloud computing, edge computing, and future generation networks). AVs have eased transportation and made significant healthcare, military, space computing, agriculture, and supply chain management. In all of these domains, AVs assist humans in performing various tasks. However, these vehicles are error-prone, and many accidents are observed in recent times [1], [2]. The complexities of AVs and their subsystems increase vulnerabilities that unethical practices can easily exploit. For example, compromised or hijack communication links, cyber-attacks and threats, and SQL injection attacks. To address these concerns that need to ensure robust and

secure solutions for an autonomous system. Compared to traditional security approaches, Blockchain technology can answer these concerns because of its security properties like immutability, decentralized and distributed network approach, transparency, enhanced security using cryptography primitives, robust consensus-building system, and faster transaction settlements, and many more. Nowadays, applications such as autonomous vehicles implementing blockchain for data security may eventually replace existing centralized security and storage systems due to blockchain's ability to provide data transparency, immutability, and decentralized storage. The most apparent application area appears to be the use of blockchain for data security. Blockchain, synonymous with trust, privacy, and security, is being investigated for a wide range of applications that require data storage that is securely encrypted and quickly recoverable. Blockchain has many advantages over traditional security solutions, some of which are as follows:

- Traditional data security and storage mechanisms are incredibly centralized, implying a single point of failure. This means that any external malicious attack on a central server, such as an attempt at brute-force hacking or malware, can result in complete or partial information loss. Information loss can be dangerous for AV-based businesses and even entire economies, depending on the type of data stored on the system. Blockchain-based storage is impenetrably secure against hacking and other external attacks. Since the same data is saved on all blockchain nodes, data loss is very low. This means that data protection and storage on the blockchain are perfect for sensitive information such as autonomous vehicle communication and user identification.
- The integrity of the data recorded on the blockchain is critical. It is practically impossible to access and edit anything stored on the blockchain without being informed and obtaining consensus from the entire network. As a result, participants can use the blockchain as a source of truth and operate a trustworthy, secure ecosystem, that is, without the need for the other party to trust or be familiar with them.
- Blockchain technology establishes a decentralized, transparent system, which creates trust among network participants. AVs can include insurance partners or workshops that form a consortium using blockchain technology to record transactional data and other shared information. Due to this nature of the blockchain, all users have equal access to the stored data, and any change requires the consent of all participants.
- Each participant in the blockchain-based network keeps the distributed ledger up to date by maintaining, computing, and updating new entries. All nodes communicate with each other, which ensures internal security. It allows you to trace the origin, record, and ownership of the data. The blockchain lets the user see how timestamps and cryptographic proofs were used to replace old and new versions of the same content.
- Any entry made in the blockchain is irreversible. Due to the decentralized nature of blockchain, the ability to update data is not centralized, whereas traditional data storage systems are centralized due to their client-server architecture. Blockchain technology maintains an immutable chain of records and transactions while retaining the previous block of data permanently. This ensures that the origin of each new block can be independently authenticated and tracked throughout the chain's history.

Blockchain technology can ensure private communication among parties [3]. The employment of strong hash functions, cryptographic primitives, privacy management, data immutability, decentralized data availability, the interaction between different AV systems, transparency in record availability, and a robust consensus technique make AV Zone safer. As a result, the chances of vulnerabilities, attacks, threats, and loopholes get reduced in infrastructure supporting AVs operations. The Blockchain system uses multiple consensus mechanisms, such as proof of work (PoW), to prevent malicious access, sybil attacks and tamper-proof the blocks [2]. Blockchain enables complete transaction transparency and immutability, which means that data is permanently published in a distributed ledger and cannot be deleted or modified. Furthermore, anonymity, security, and the absence of a third party are all additional advantages to the application using blockchain. If one person solely keeps the ledger, there is a chance that mistakes will be made, either accidentally or deliberately. Thus, everyone in the network maintains the ledger, and it becomes difficult to cheat. As a result, the network's vulnerabilities are mitigated by its transparency and immutability. Additionally, blockchain technology would help create multiple independent distributed ledgers, securing data associated with numerous stakeholders. For example, numerous blockchain networks for drivers, cars, traveling plans, road-maps, and satellite-based communication can ensure maximum system security. As a result, the chances of error or on-road accidents can be reduced to a minimal level.

A. INTRODUCTION TO BLOCKCHAIN TECHNOLOGY FOR AVs

The rapid transformation of blockchain from a theoretical concept to practical reality is notable. From healthcare to food supply chains, blockchain is currently revolutionizing many fields. Millions of IoT devices must interact and transfer data instantly in the era of AVs, and these exchanges of data should be transparent and shareable. Blockchain is a decentralized network that ensures the tampering of data, impossible, allowing for secure, private, and quick transactions. Vehicle manufacturers have already imagined: how autonomous technology can improve AVs, increase customer satisfaction, customer retention, and overall auto experience. With the maturity of blockchain and growing demand for AVs, digital identities such as vehicle identification, ownership, warranty, wear and tear, leasing, lending, parts

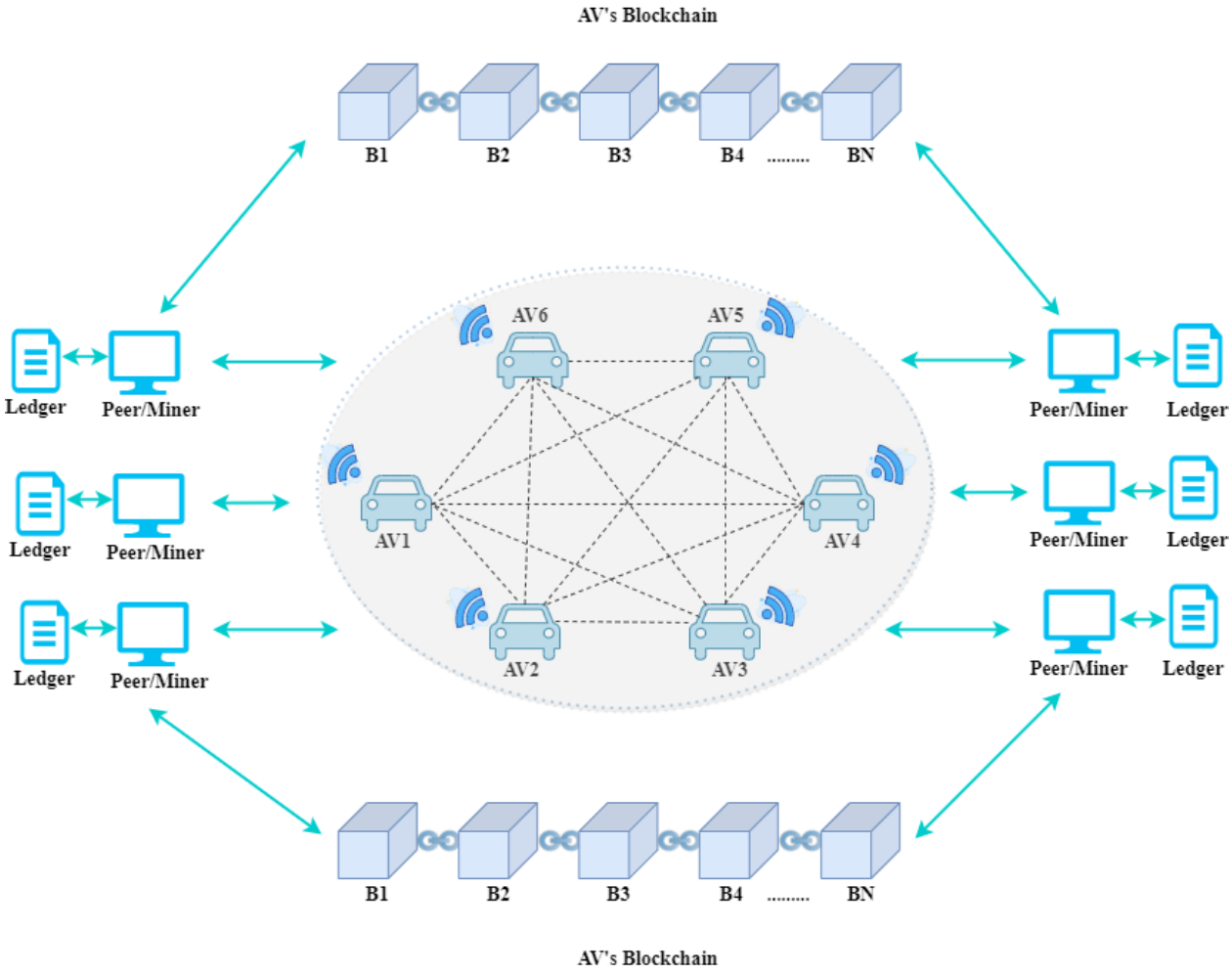


FIGURE 1. Blockchain network of autonomous vehicles.

management, storage, transfer, and servicing information are being investigated. This data will be recorded in a shared ledger structure using blockchain technology and smart contracts. Authorized parties will have access to a part of the data in this ledger which depends on their usage rights and requirements. As a result, vendors, executives, and other organizations will authenticate and use certificates in near real-time [4], [5].

Blockchain is a secure, ever-growing, and shared record-keeping approach whereby a copy of the record is kept by each user of the data and can be changed only if all participants in the transaction agree to the update. It means that a blockchain is a P2P distributed record that is cryptographically secure, immutable (very difficult to edit), append-only, and can only be updated by peer consensus or agreement algorithms. Virtually anything can be recorded and distributed on a blockchain network to reduce risk and costs for all involved parties. Blockchain technology can enable decentralized, P2P transactions, increase data integrity and robustness, and provide reliable digital identities for vehicles, components, and customers [6]–[8]. It is accomplished using a selection of techniques, including:

- Reading and writing encoded transactions as blocks of chronologically linked data by hashing methods helps prevent data tampering or erasure.
- The blockchain network uses a consensus algorithm to synchronize distributed data between network participants, creating a decentralized and immutable record.
- The data is shared between several participants through a distributed ledger, which minimizes the points of failure.
- Allowing authorized parties and their certified users and assets facilitates value transfer to people without traditional intermediates.

Figure 1 shows the blockchain-based architectural network for AVs, in which all vehicles (AV1-AV6) are connected to IoT sensors. These sensors help the autonomous vehicle and driver control, monitor, instruct, direct and guide based on their service requirements. Miner nodes are responsible for authenticating the trust of the rest of the nodes or IoT devices, while peer nodes are a part of the overall blockchain. Now, if the communication and transmission ranges are high, it can help the autonomous vehicle, driver, or system connect to many vehicles. In this connectivity, blockchain plays a vital

role. Blockchain technology can help to track and record vehicle activities. It has the power to authorize a particular set of legitimate users only or authorize a specific group of illegitimate users. The data of a vehicle and its activities can be collected from customers or users using IoT sensors. An attack can tamper with an IoT sensor as well. Since blockchain is observing activities, it would be easier to identify such attackers, and the necessary actions (pre-defined) can be taken timely. This will stop the compromise of IoT sensors.

B. BLOCKCHAIN SOLUTIONS FOR AVs

In recent times [9], [10], various studies proposed integrating blockchain technology with AVs. For example, Pokhrel and Choi [10] proposed a blockchain-based design for AVs. This design uses FL to ensure data privacy and improving the efficiency of vehicular communication, as well. Here, a mathematical framework is proposed. This framework helps in developing a controllable network using blockchain and FL parameters. These parameters include block size, block arrival rate, data retransmission limit, and frame size. This work has identified various challenges in the proposed model that need futuristic investigations. For wireless connectivity-based vehicle tracking systems, advanced mobility models. There is a shortage of mobility awareness, efficient verification poses a forking problem, and privacy leakage risk analysis is necessary Shivers *et al.* [9] proposed a framework for a decentralized ride-hailing platform. This platform is used in AVs for improving the riding experiences. This work presents the implementation and analysis of the proposed framework using multiple tools under varying network loads. Likewise, various blockchain integrated solutions are offered for automated vehicles [11]–[21]. Table 1 shows the comparative analysis of recent studies that proposed blockchain technology for automated vehicles.

C. MOTIVATION AND RESEARCH PROBLEM

Following are the critical research motivation and research problems in this work.

- Presently, many efforts are drawn to streamline processes and improve the autonomous experiences and methods in modern vehicles. Usage of advanced technologies (IoT, AI, ML, Blockchain) has shown a significant improvement over the current techniques in bringing efficiency, usefulness, and transparency in various applications. However, very few studies have focused usage of blockchain in autonomous vehicles. Thus, there is a need to explore autonomous vehicles, their properties, and their classifications. Further, the importance of blockchain technology to autonomous vehicles, its cyberspace, and systems are important to realize.
- Autonomous vehicles need real-time responses to events. In such cases, blockchain technology-based smart contract plays an important role. Blockchain technology ensures strong interconnections and smart contracts execute transactions based upon circumstances. Thus, it is important to identify the needs of intelligent contracts in handling autonomous experiences in modern vehicles.
- There are different types of autonomous vehicles like AGV, AEV, AUV, UUAV, and AAeV. All of these autonomous vehicles have different categories of vehicles. Thus, it would be interesting to explore the major classes of these autonomous vehicles and study the importance of blockchain technology to them.
- In autonomous vehicles, blockchain-based distributed networks can be created for individual subsystems and whole system operations. For example, AEV consists of charing, storage, data processing, power, and waste management systems. A blockchain network can be created to integrate all of these systems. Individual blockchain networks can be made for each subsystem, and advanced blockchain concepts (bridge and side blockchain) can be integrated into one system. Thus, it is important to understand the importance of each subsystem (with example) and how they can be combined to provide flawless autonomous experiences.
- In addition to a subsystem or system integration using blockchain technology, blockchain is helpful in autonomous vehicle usage in various applications. For example, AGV is used in supply chain management in multiple warehouses across the globe. Thus, exploring their use in applications' importance, usage, efficiency, and model would be interesting.

D. CONTRIBUTIONS

The contributions of this work are briefly explained as follows.

- This work explores the recently developed AVs, their types and performs a comparative analysis of features.
- To understand the importance of blockchain technology in AVs and study those recent proposals that integrated both technologies.
- This work identifies the characteristics that are important to understand the significance of blockchain in autonomous vehicle systems.
- This work lists and compares the challenges discussed in those recent studies that propose blockchain solutions for AVs.
- This work discusses the blockchain technology integrated use cases for automated vehicles like automated guided vehicles.

Figure 2 explains work organization.

II. THEORETICAL BACKGROUND AND SURVEY PREPARATION

This section briefly explores the literature review or background on recent developments, surveys, and practices over blockchain technology for AVs. It shows the significance and

TABLE 1. Comparative analysis of blockchain-integrated autonomous vehicle systems.

Author	Year	A	B	C	D	E	F	G	H	I	Application	Key Finding
Guo et al. [13]	2018	✓	×	×	✓	×	×	×	✓	✓	An event recording system with blockchain technology support is proposed for autonomous vehicles.	In this work, a dynamic federation consensus algorithm is verified and tested for autonomous vehicles. Further, security analysis is also performed.
Shivers et al. [9]	2019	✓	×	×	✓	✓	×	✓	×	✓	Blockchain-based Ride-hailing platform	Performance is measured using static analysis tool and it is observed that system works properly under heavy network load.
Baza et al. [11]	2019	✓	✓	×	✓	×	×	×	✓	✓	Firmware update scheme to control, monitor and data manipulation operation is proposed.	Secure firmware update scheme is proposed for autonomous vehicles that leverages the gaps between blockchain and smart contract for futuristic vehicles.
Saini et al. [18]	2019	✓	×	×	✓	×	✓	×	✓	✓	Blockchain-technology-based secure priority vehicle movement and control system is proposed.	This work discusses the message process flow for connected vehicles and priority services for priority vehicle.
Ayvaz and Cetin [15]	2019	×	×	×	✓	✓	×	✓	✓	✓	A record keeping system with blockchain technology for autonomous vehicle movement in untrusted environment is proposed.	In this work, blockchain protocol-based record keeping system is proposed to monitor and operate the autonomous vehicles. The proposed system is capable of defending against attack and helps the vehicles to move and co-operate safely in untrusted environment.
Yang et al. [23]	2019	×	×	×	×	×	✓	×	✓	✓	Surveyed the importance and technical features of automated underwater docking.	This work has prepared in-depth features and framework methodologies for autonomous underwater vehicle docking with maximum safety and long-duration operations.
Shrestha et al. [12]	2020	✓	×	×	✓	×	✓	×	✓	✓	A survey over blockchain and 5G-based solutions for vehicular networks.	This work investigates the security, privacy protection and content caching for blockchain and 5G technologies-based solutions to vehicular network.
Wang et al. [16]	2020	✓	×	×	✓	✓	✓	×	✓	✓	Proposed a system with secure and incentive content delivery for integrated connected autonomous vehicles.	A mathematical and theoretical discussion is developed over content delivery in blockchain-enabled integrated connected autonomous vehicles. A simulation-based system is proposed for decentralized permissioned network.
Jiang et al. [17]	2020	✓	×	×	✓	✓	×	✓	✓	✓	Proposed blockchain-enabled scheme for object detection and information sharing in cross-domain adaption for autonomous driving with improved performance.	This work has integrated the blockchain and mobile-edge computing technology for reducing the domain discrepancy in object identification and categorization. Blockchain is used to improve the reliability and smart contract to ensure secure data storage, accessibility and task sharing.
Jiang et al. [14]	2020	✓	×	×	✓	✓	×	✓	✓	✓	A video analytics framework is proposed. This framework consists of edge computing, blockchain and internet of autonomous vehicles for optimum solution.	In this work, blockchain technology, multi-layered edge computing, federated learning, internet of things and video processing is proposed for optimum automated vehicle system. This system improves the performance and provides fast and secure framework.
Alladi et al. [19]	2020	×	✓	×	✓	✓	×	×	×	✓	Reviewed blockchain applications for unmanned aerial vehicle for security, data storage, inventory and surveillance.	Discussed the detailed review over multi-layered blockchain architecture for unmanned aerial vehicles used for security, inventory and surveillance. This is a detailed survey of blockchain and aerial vehicle usage, challenges and possible solutions.
Megha et al. [20]	2020	✓	×	×	×	×	✓	×	×	×	Conducted a short survey of autonomous vehicles mainly discussing the recent studies, applications and future.	This is a brief survey that gives introduction to autonomous vehicles, various levels of autonomous driving experiences, key features, challenges and brief solutions.
Fu et al. [21]	2020	✓	×	×	✓	✓	✓	×	✓	✓	Surveyed blockchain and AI-enabled connected and autonomous vehicles.	This work has surveyed the importance of blockchain technology for connected and autonomous vehicles. A framework is presented and ways to utilize the collective intelligence is proposed using machine learning models.
Pokhrel and Choi [10]	2020	✓	×	×	✓	×	×	✓	✓	✓	Federated learning and blockchain-based system for autonomous vehicles	On-vehicle machine learning model with proof-of-work and mathematical framework with minimum delay for autonomous vehicle is proposed in this work.
Yang et al. [23]	2021	×	×	✓	×	×	×	×	✓	✓	This work surveyed automated underwater vehicles, its formation control and underwater acoustic communication capabilities.	In addition to automated underwater vehicle survey, a framework is proposed that provides a comprehensive classification method for underwater automated vehicles. This framework can be used for communication-related formation selection for different applications.

A: Blockchain network development for automated vehicles, B: Cryptocurrency usage, C: Underwater Automated Vehicles, D: Blockchain-based Security Concerns, E: Blockchain-based Data Handling, F: Survey to discuss blockchain integrated solutions for automated vehicles, G: Blockchain-based platform or tool for automated vehicles, H: Automated vehicle coordination issue discussion or solution, I: Performance, security or QoS

need of blockchain technology for AVs. Details of similar studies are explored in subsequent sections. Further, this section presents the research methods followed in the survey and the process, from article selection to key finding observation and discussions. Details are explained as follows.

A. RECENT SURVEYS OVER BLOCKCHAIN TECHNOLOGY FOR AVs

This sub-section explains the recent blockchain technology and autonomous vehicle developments and their integration studies. Details are presented as follows.

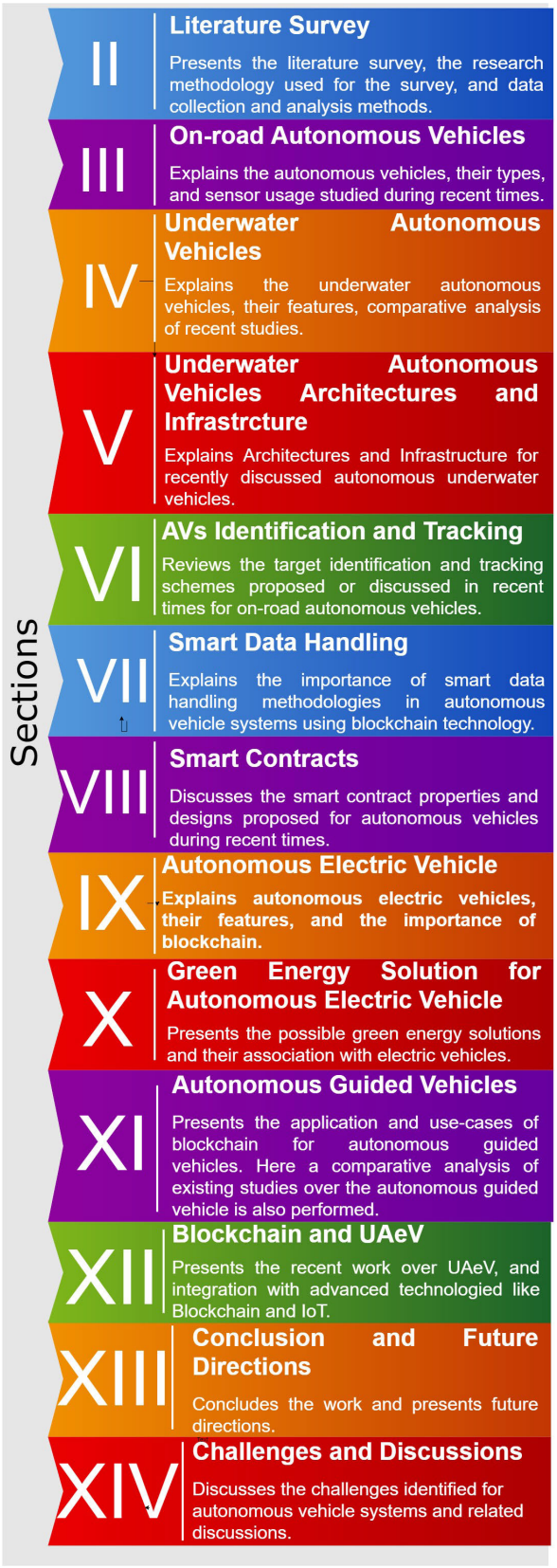


FIGURE 2. Work organization.

- Mariani *et al.* [22] realized the importance of coordination of AVs and self-driving vehicles in nearby times. In this work, critical classes of coordination are introduced. After that, challenges and solutions are proposed that efficiently handle the coordination issues. Future research challenges focus on dynamic switching in coordination schemes, ethical issues, single or multi-lanes car operation, driving intersections, road neutrality, and multiple car types and pedestrian interactions. Although significant concentration is drawn towards coordination issues, blockchain technology for events recording and data handling is not discussed. Likewise, the importance of decentralized networks (especially blockchain-based networks) and security enhancements are not explored in detail.
- Yang *et al.* [23] conducted an in-depth survey over automated underwater vehicles. This work has proposed a classification framework for automation control selection and classification for various applications. The major categories of automated underwater vehicles identified in this work include biometric, underwater gliders, and torpedo shape vehicles. After performing the comparative feature analysis, it has been determined that the torpedo vehicle has balance performance, the biomimetic vehicle is lightweight, and underwater gliders can travel to thousands of kilometers irrespective of their comparatively slow speed. This survey is an in-depth survey covering underwater vehicles. However, blockchain or related aspects are not touched upon in this article. To keep the records of underwater vehicles immutable, transparent to the network, and secure, blockchain aspects are necessary to explore. They are likewise, Examining the importance of smart contracts, distributed ledgers, and consensus mechanisms for multiple underwater vehicles, their coordination, and a transparent process to conduct transactions on a pay-per-event basis.
- Yazdani *et al.* [24] discussed the importance of UAVs and their long-endurance operational capabilities. Here, underwater vehicle's docking methodologies, merits, shortcomings, and guidance to operate with high performance are discussed. In this work, an in-depth technical review is conducted to present the (i) existing methodologies and equipment, (ii) challenges in attaining a safe docking using a simple scenario, (iii) discuss the requirements of general-purpose guidance framework and show the need for calculus of variations method for automated underwater vehicle's docking. This work needs to extend the importance of docking with blockchain. The usage of the docking station, its facilities, and its long-term use can be ensured and transparent. Likewise, system features stored in a distributed ledger for monitoring and surveillance can be identified and programmed to track the assets and monitor their performances.
- Shrestha *et al.* [12] conducted a comprehensive survey over blockchain solutions to ensure security in V2X connectivity. The security aspects are provided through 5G

and blockchain-technology solutions, and discussions are developed over integrations. Among open issues, storage requirements with increased vehicular network scalability, performance in terms of throughput and network resource utilization, and blockchain incentive mechanisms for efficient build-up are proposed. This work needs to be extended with different categories of attacks occurring in the blockchain network. For example, the feasibility and countermeasures for 51% of attacks, jamming attacks, physical attacks, cyber-attacks, hijacking attacks, identity, and privacy concerns, and communication link failure or unethical control need to be explored in detail.

- Wang *et al.* [16] discussed the blockchain technology solution for secure content delivery in vehicular social networks. Here, the PoR consensus protocol is designed and concerned for vehicular social networks within a multi-party scenario. A safe delivery ratio-based analysis is computed by varying the simulation time. The results demonstrate that the proposed approach is efficient compared to the conventional method. This work needs attention over the high cost of autonomous vehicles, which may increase further with the integration of blockchain technology. Additionally, attack detection and resistant strategies need to be explored to ensure a system with high quality and better performance.
- Jahan *et al.* [3] prepared an in-depth analysis of attacks and vulnerabilities in autonomous systems. This work has prepared attack classifications and theoretical discussions over the development of autonomous systems in recent times. Multiple AVs, their features, and recent developments are discussed. This survey has explained the attacks in-depth with examples. Particular focus is on system modeling threat and vulnerability modeling attacks—the extended analysis of attacks for assets with different capabilities. For example, a network may consist of resourceful, resource constraint, hybrid or unknown devices. Thus, how blockchain networks, attack analysis processes, monitoring and countermeasures will be helpful to ensure a safe autonomous system and an exciting challenge to explore.

Likewise, various studies are observed during recent times that focus on AVs, autonomous systems, UAVs, AGVs [1], [2], [25]–[36]. These surveys discuss the importance of autonomous systems and technologies in present times and from futuristic perspectives. It has been observed that these systems (with variable automation levels) are widely implemented in various applications and services to assist humans in improving working conditions and environments. However, most existing methods cannot ensure full integration of blockchain technology for various reasons like cost, performance, and efficiency concerns. Table 2 shows the comparative analysis of blockchain-integrated autonomous vehicle systems surveys.

B. RESEARCH METHODS

To study and identify the significant challenges and solutions of blockchain technology, AVs, and their integration methodologies as follows [4], [5], [9], [12], [15], 20], [22], [25].

- This work has thoroughly browsed the literature to identify existing blockchain technology-based AV systems and proposed approaches. In addition, this work discusses recent ways of applying blockchain technology to improve autonomous vehicle experiences. And, action is taken for design or study and feature-based analysis.
- This work has explored different AVs and discussed the importance of blockchain technology in handling data security, coordination, and distributed decision-making issues.
- Consequently, the use-cases of AGVs in the industry are discussed. The industry background and experience of one of the authors is utilized to prepare three sets of use-cases. These use-cases discuss the importance of blockchain technology for automated guided vehicles, key challenges, solutions, advantages, and disadvantages in a real-time environment.

C. DATA COLLECTION AND ANALYSIS

This section briefly explains the process followed, starting from article collection to survey preparation. Figure 3 illustrates the procedure followed to prepare this survey. This process follows the following important three phases:

- ***Article Collection:*** This phase of the process includes a literature search. In the literature search, the following number of articles are selected from reputed publishers: 32 (Elsevier), 31(IEEE), 41 (Springer), 10 (ACM), 8 (Wiley), 5 (Taylor and Francis), 2 (Hindawi), 2 (SAGE), 2 (MDPI), 2(IET), and 30 (Others including web-references). The keyword-based search was applied in search engines (mainly the publisher search engine or google scholar). The keywords include: ''blockchain for AVs,'' ''blockchain for guided vehicles,'' ''blockchain for underwater vehicles,'' ''autonomous vehicle surveys,'' ''blockchain surveys for AVs,'' ''blockchain in autonomous driving,'' ''AVs,'' ''underwater AVs,'' ''guided vehicles,'' ''use-cases for autonomous,'' and ''smart contracts for AVs.'' Each author has prepared their article dataset (or repository) and stored it at the central warehouse.
- ***Article Analysis:*** In this phase, a theme table is prepared by every author. This themed table includes key findings from the literature survey (or known as a survey-type), practitioner-based article (or known as implementation-type), and industry-specific (white papers, websites, and author's industry experience). Authors have prepared the theme tables on the following topics***:*** **(i)** AVs and types, (ii) UAV, (iii) target identification and tracking schemes in AVs, (iv) intelligent data handling methodologies for AVs, (v) smart-contract design for AVs, (vi) AEV, (vii) green energy solutions for electric

TABLE 2. Comparative analysis of blockchain-integrated autonomous vehicle systems surveys.

Author	Year	A	B	C	D	E	F	G	H	I	J	Major Survey Directions	Major Survey Shortcomings and Challenges
Jahan et al. [3]	2019	×	✓	✓	✓	✓	✓	×	✓	×	×	This is an in-depth observation of autonomous systems. In this work, multiple autonomous systems are covered. An in-depth analysis of security concerns, attacks, vehicle types, usages, system modeling, blockchain usage and trust management are discussed.	This work can be extended to design blockchain and smart contract-based use-cases for autonomous driving, vehicles and systems. To reduce the accidents and attack probabilities, system design, formal, simulation or implementation-based observations are necessary in near future.
Wang et al. [16]	2020	✓	×	✓	×	×	×	×	✓	×	×	This is a short survey and analysis article on investigating the content delivery system in autonomous vehicular social networks. Systematic discussions are developed over autonomous vehicular network enhancements and social network creation for important applications.	The consensus protocol designed for efficient deployment of blockchain network and content delivery systems are limited to vehicular social networks rather than exploring it for fully autonomous vehicle network.
Megha et al. [20]	2020	✓	×	✓	×	✓	×	×	✓	×	×	Discusses the quality attributes for blockchain-based autonomous vehicles. This include human safety, data security, privacy, transparency, reliability and efficiency.	Very generic discussions are developed to integrate blockchain technology for autonomous vehicles. The rapidly expanding domain is expecting in-depth discussions.
Fu et al. [21]	2020	✓	×	✓	✓	×	×	×	✓	×	×	This is a short survey article on connected and autonomous vehicles. This work proposes cloud-infrastructure-based single vehicle intelligence, centralized, and distributed approach for connected and autonomous vehicle movements.	The addressed problem of data storage in connected autonomous vehicle can be extended to applications like warehouse-based system consisting of automated guided vehicles. Likewise, the proposed approach can be tested for various other applications.
Shrestha et al. [12]	2020	×	✓	✓	✓	✓	×	×	✓	×	×	Discuss the evolution of vehicle ranging to everything, the connectivity, integration of edge computing, challenges in integrating 5G, Blockchain and Edge-based infrastructure for autonomous vehicles, and open issues and research challenges.	No smart contract and blockchain-integrated framework is proposed or no such use case is discussed to smartly handle the data for vehicular networks. Proposal is made for generalized autonomous vehicles.
Proposed Survey	2021	×	✓	✓	✓	✓	✓	✓	✓	✓	✓	The current work discusses the autonomous vehicle concept thoroughly. This is a broad and in-depth survey over different autonomous vehicle aspects. Blockchain discussions are developed in parallel.	Integration of multiple advanced technologies and related studies are not explored in this work. For example, need of cloud computing, data storage architectures, cryptography features are not discussed. These aspects will be taken up in future.

A: short survey, B: Long and in-depth survey, C: Driver Assistance-based System Discussion, D: Fully Autonomous Vehicle Discussion, E: Partial Autonomous Vehicle Discussion, F: Automated Underwater Vehicle, G: Automated Guided Vehicle, H: Blockchain proposal discussions, I: Electric Vehicle Discussions, J Green Energy Solution Discussions.

vehicles, and (viii) use-cases for blockchain technology in AGVs. These theme tables are selected as significant sections of this work and are explained in the subsequent section.

- ***Synthesis and Evaluation:*** In addition to the theme preparation in the previous phase, another set of theme tables are prepared that classify the articles based on autonomous vehicle features, research practices, implementation practices, case studies, and theoretical discussions. The comparative literature analysis is drawn mainly using these theme tables. A detailed explanation of selected themes and other findings are explained in subsequent sections.

III. AVS LEVELS, SENSORS, AND BLOCKCHAIN

An autonomous vehicle can sense its environment and operate without human intervention. The human passenger is not necessary to manage the vehicle, and the human driver is not essential to sit in the vehicle. Ultrasonic sensors, RADAR, LiDAR, GPS, motion and angle sensors, cameras, inertial units, and audiometry are technologies used by autonomous cars to observe the environment. Advanced control systems analyze sensory data to determine the best navigation routes and obstacles and appropriate signage. [37], [38].

A. SENSOR FUSION FOR AUTONOMOUS DRIVING

Sensor fusion combines data from several sensors to produce a much superior result in using each sensor separately. In the field of AVs, sensor fusion is one of the most crucial subjects. A fused sensor device incorporates the advantages of individual sensors to hypothesize about the state of the vehicle's atmosphere. Fusion algorithms allow a vehicle to determine how many obstacles are present, where they are located, and how quickly they are going. However, the best mix of sensor fusion algorithms will take autonomous driving to a new level of safety and address various concerns [39]. For example, the elimination of human error by connecting our road infrastructure with the sensors like RADAR, motion and angle sensors, and LiDAR [40]. As a result, traffic safety and reduction in accidents can be ensured. Each of these sensors has several advantages and drawbacks. Sensor Fusion seeks to tap the potential of each sensor to gain a deeper

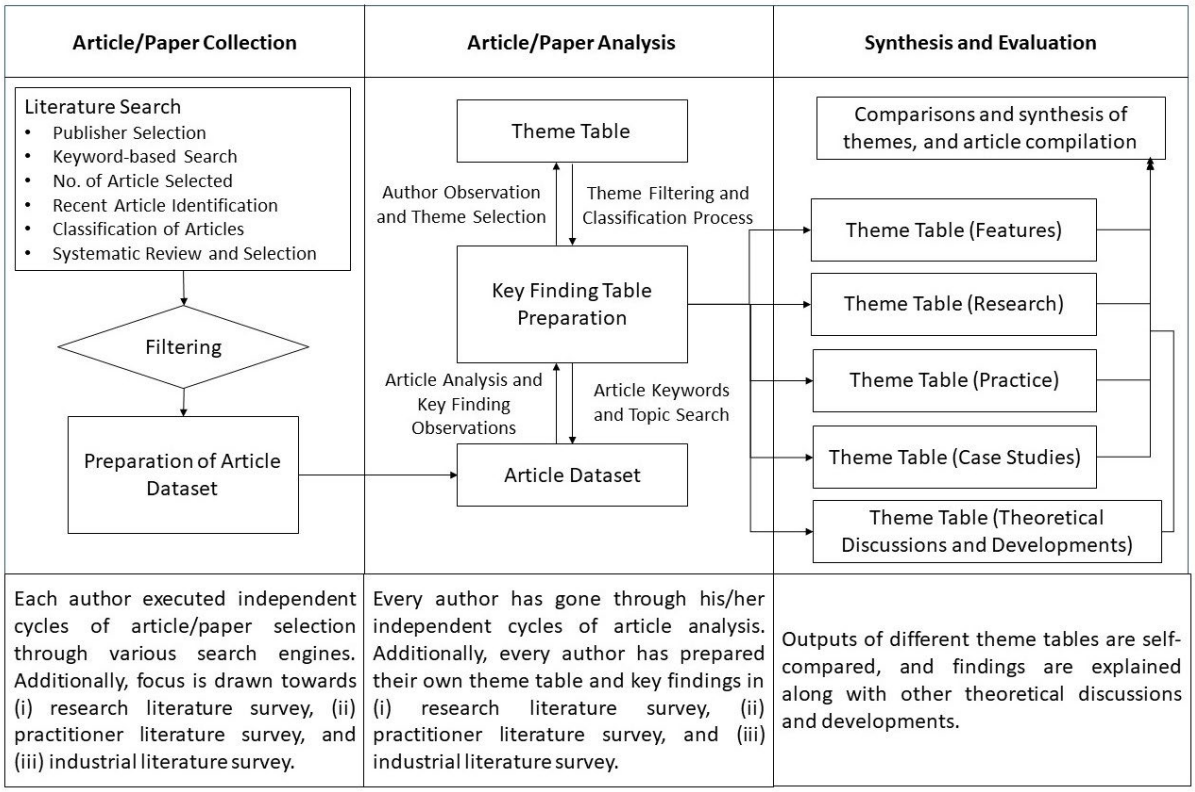


FIGURE 3. Process involving article collection, analysis, synthesis, evaluation, and survey preparation.

understanding of the environment. Using the camera, you can search roads, read road signs and identify vehicles. The LiDAR system can better predict the vehicle's position, while the RADAR system can better estimate the vehicle's speed. An autonomous vehicle (shown in Figure 4) uses many sensors fused to analyze, detect and maneuver its environment. Table 3 shows the specifications of various sensors used in autonomous vehicles.

Vehicle numbers, driver information, path conditions, environmental information, insurance, and maintenance information obtained by the IoT sensor fusion network depicted in figure 4 are kept in a distributed ledger and blockchain network to track and record authorized and illegal conduct of the vehicle. IoT enables devices on the Internet to send data to a blockchain network to create a tamper-resistant record of shared transactions. Transactions are timestamped and incorporated into cryptographically secure blocks through a hashing process after the blockchain network's validation. The hash method links the blocks together to form a sequential chain. The use of blockchain in IoT can reduce single points of failure while also providing a secure and efficient way to store and process IoT data. The peer-to-peer design of the blockchain is seen as a potential solution to challenges with a single point of breakdown and bottleneck. If an IoT sensor is tampered with by attackers, the proper blockchain authorities can identify the compromised IoT sensor and take swift action against them. Blockchain ensures the integrity and authenticity of data transactions and events by using immutable hash values and digital signatures. In short, blockchain enables users to observe network transactions to protect computer and data rights. Sensors that can reduce human error and improve infrastructure facilities are briefly explained as follows.

- ***Motion and Angle Sensors***: The motion sensors measure acceleration in the longitudinal and vertical axes to monitor the speed of the wheels and communicate this information to the driving system [41]. Steering angle sensors determine the location of the front wheels. When compared with other data, the dynamics of AV can be measured. If geolocation deteriorates or disappears (e.g., going into a tunnel loses or weakens the signal), then data from motion and angle sensors are combined to form a solution, known as "dead reckoning" [42].
- ***LiDAR Sensors***: The best sensor used in AV is LiDAR. A laser beam emits light waves that travel at the speed of light to distinguish nearby targets. The difference in laser return time and wavelength is used to create a digital 3D image of the target environment and indicate its position within a 4-inch radius. It can also isolate single droplets of rain under single molecules using single and multiple scan lines and an array of levels unaffected by other sensors [43]. This sensor can also calculate the vehicle's height, speed, and direction, and it fits with any current safety characteristics.
- ***Ultrasonic Sensors***: Ultrasonic sensors can be necessary for the safety of a self-driving car. They use time echoed

TABLE 3. Specifications of various sensors used in autonomous vehicles.

Sensor Type	Signal type	Working range	Usage
Light Detection and Ranging (LiDAR) Sensors	Infrared	Mid and short-range	Object Detection, Object classification, Light Detection, and Ranging, collision avoidance
Ultrasonic Sensors	Ultrasound	Proximity	Parking assistance
GPS Sensors	Microwave	Global	Navigation
Cameras	Visible Light	Long, mid, and short-range	Object classification and interpretation, detect road signs, traffic lights, lane detection
Radar	Microwave	Long and short-range	Adaptive cruise control, Object detection, Radio Detection and Ranging, collision avoidance

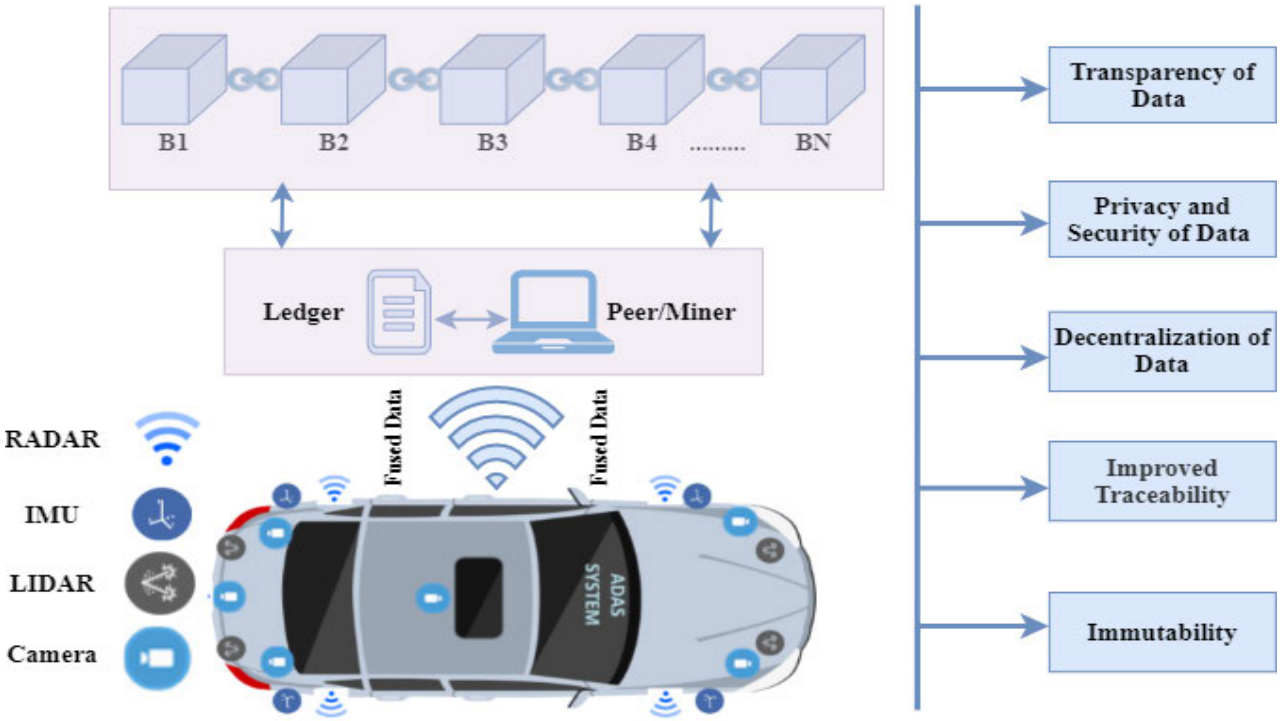


FIGURE 4. Benefits of blockchain with sensor fusion data.

by sound waves to mimic bat navigation depicting adjacent surfaces. The sensors will use this information to determine how far away the objects are and warn the vehicle's onboard system as they get closer. They are ideal for low-speed, small to medium range applications such as lateral movement, blind-spot tracking, and Parking because they use sound waves of higher frequencies than detectors for the human ear [44].

- ***GPS Sensors***: The GPS sensor receives geolocation and timing information from a satellite-based navigation system. If you have an uninterrupted sight of four or more satellites, your position can only be indicated by a few meters [45]. While it is necessary to move from point A to point B, it will be inadequate on its own due to weather conditions. Combining data with other sensor data enables it to play an essential role in synergy.
- ***Cameras***: The ability to correctly detect and discriminate between stationary and moving obstacles in the environment is vital to secure autonomous driving. The use of camera sensors is a cost-effective approach to self-driving car safety [46]. Rear and 360-degree cameras are often used to provide images of the environment in a car. Stereo vision is a two-dimensional and three-dimensional approach that we can see through our eyes. The data from these sensors allows the vehicle to precisely determine the distance between nearby objects and those far away. Infrared vision improves this ability by detecting a thermal or heat signature that will distinguish humans and things. It is necessary to see the temperature difference on the road surface and alert the AV.
- ***RADAR:*** The RADAR sends out radio waves to detect objects within a few meters. Over the years, we have

installed RADARs in our cars to track vehicles in blind spots to prevent accidents. They do better on moving objects than static objects. Unlike other sensors that determine the difference in direction between two readings, the RADAR uses the Doppler effect to determine whether the car is moving toward or away from us by calculating the change in the subsequent wave frequency [47].

B. LEVELS OF DRIVING AUTOMATION AND BLOCKCHAIN

There are many degrees and classifications for a fully automated driving system in an autonomous driving vehicle, enabling the appliance to be repaired if its components fail. We have a different set of classifications now coexisting for AVs, but those standards do not change much from each other. The SAE [48] has designed a harmonized framework to describe six degrees of autonomous driving. SAE is characterized by 6 degrees or levels of driving Automation i.e. 0 (completely manual) to 5 (completely independent) [49]–[51].

1) NO DRIVING AUTOMATION (MANUALLY CONTROLLED)-LEVEL 0

Nowadays, most vehicles on the road are manually controlled or level 0. The automated system provides alerts and may interfere for some time but does not have long-term vehicle control. Users have complete control over your vehicle at level 0. For example, when you back up and move too close to another vehicle, your vehicle may sound a warning, such as an audible warning, but you must activate the brakes to avoid hitting the other vehicle. Blockchain plays a minor role in this automation level. Suppose blockchain technology is integrated with the vehicle at this level. In that case, it can help give the vehicle and its states information to be stored in a distributed ledger for constantly monitoring the vehicle's performance.

2) DRIVER ASSISTANCE (HANDS-ON)-LEVEL 1

It is the minimum degree of automation. Level 1 vehicles are equipped with a single automatic system that assists the driver with acceleration or steering (cruise control) tasks. ACC, which permits the vehicle to maintain a safe gap behind the following vehicle, passes as Level 1. The human driver monitors other aspects of steering controls, such as driving and slowing down. At this level vehicle is controlled by both the driver and the automated system. For example, vehicles in which the driver has complete control over the steering.

In comparison, automatic systems adjust engine power to keep a set speed or engine and brake capacity in response to speed changes. Additionally, there exists parking assist, in which steering is automatic, with speed manually managed. As compared to level-0, take more blockchain advantages at level-1. At this stage, more data, including information about a single automatic system, can be added to the distributed ledger. In this way, blockchain will help in ensuring security, immutability, and transparency to vehicle operations.

3) PARTIAL DRIVING AUTOMATION (HANDS OFF)-LEVEL 2

The vehicles can steer and speed control and the highest degree of end-user automobiles equipped with an autopilot. While the supervising driver system permits the driver to ''hand-off'' the steering wheel, the driver cannot sit ideal; he is still accountable to the vehicle. He must maintain constant driving-related attention. At this stage, the vehicle is capable of steering as well as accelerating and decelerating. Here the automation is similar to self-driving in that it occupies the driver's seat and can command the vehicle at any time. Blockchain integrated with level-2 automation can ensure more data availability and security compared to level-0 or level-1. At level-2, autopilot and vehicle information are made available over the blockchain network. For example, ''Hands Off'' operation observations can be recorded and stored in the distributed ledger. Continuous availability of this operation can help in rating the autonomous vehicle's experiences.

4) CONDITIONAL DRIVING AUTOMATION (EYES OFF)-LEVEL 3

Level 3 technology eliminates the need for drivers to keep their eyes on the steering wheel or the road to keep the vehicle stable on the road. Instead, users can use the smartphone to read messages, watch movies, and play games. The only condition is that you stay in your vehicle. Here, level 3 AVs can notify the driver to respond to situations they cannot resolve independently, such as crossing road construction locations. Level 3 AVs are capable of self-driving, but only under certain right conditions and with particular constraints, such as a limited divided highway with a restricted speed limit. A human driver is still required to take charge in the event of deteriorating road conditions. The conditional automation of the SAE classification system is the most controversial classification because it allows the driver to focus on non-driving responsibilities while ultimately being accountable. The availability of autonomous operation data over blockchain networks increases with this level. This level can ensure every other autonomous experience data to the blockchain network, except responding to real-time events.

5) HIGH DRIVING AUTOMATION (MIND OFF)-LEVEL 4

Even in terms of safety, vehicles requiring human interaction are classified as level 4 in the SAE classification system. They can perform all driving responsibilities independently, allowing the driver to rest or sleep. At this level, vehicles can drive autonomously without human assistance (except when entering their destination). The driver of a Level 4 vehicle always has complete control over the vehicle. In addition, Level 4 automobiles can manage road construction locations and other complicated scenarios if the operating conditions of the car's software are satisfied. As level-4 increases autonomous operation by one more level with provision to

sleep or rest for a driver, the availability of autonomous operations' data to blockchain-based distributed ledger increases compared to level-0 to level-3.

6) FULL DRIVING AUTOMATION (STEERING WHEEL OPTIONAL)-LEVEL 5

Most self-driving vehicles aspire to complete startup automation. Even in the most challenging settings, such as dirt tracks, human involvement is never needed at this point. In a nutshell, Level 5 cars have no driver and only passengers. On the other hand, drivers are free to take it whenever they like. In more extreme models, such vehicles can be similar to mobile living spaces, complete with a comfortable lounging area that maximizes interior space for laptops and freezers. Full automation can benefit individuals who cannot drive due to limitations such as vision or paralysis. Also, ride-sharing fleets can take passengers at lower prices because they do not have to pay drivers. As there is no driver available at level-5, the blockchain network concentrates on vehicle data only. Thus, create a specialized blockchain network for autonomous vehicle operations. This network provides safety, privacy, security, and other blockchain features and autonomous functions.

IV. UAV

The focus of the previous section was on AVs, and the subsequent section focuses on UAVs. The historical perspective, types, applications, research directions, and developments are discussed as follows.

In the seventeenth century, at Saybrook, Connecticut, the first submarine, a small-sized underwater wooden vehicle put together through metal straps, was built by David Bushnell and Ezra and named 'Turtle' [52]. This submarine was the first one to be involved in a naval battle at New York Harbor, and this paved the way for the use of many submersibles in various operations and tasks. In parallel, the development of torpedoes was observed, which can be considered truly the first UAV. In and around time, while the effect of UAVs progressed, many appeared but could not exist or sustain for more extended periods. However, successive years witnessed moderate growth in physical development and further research, making these vehicles significant in commercial scenarios.

Traditionally, underwater vehicles are classified into two classes, depending on whether they have a human directly boarding it and operating it or self-controlled with its onboard systems. Thus, the two classes are (a). operating systems, and (b). unmanned systems. Manned systems could be military submarines or non-military submarines, where the non-military ones primarily support activities involving underwater investigations and experiments. Unmanned vehicles are classified under three major classes; the first type is the simplest and towed behind a ship—these act as a platform, with various sensor assemblies attached to the vehicle frame. The second class is ROV, a tethered submarine with a remote operator controlling the tether that supplies power and communication to the ROV. The third class is UUnV, which is the most advanced type. It is untethered, has its onboard power, is linked through a communication channel, controls itself independently, and accomplishes the pre-defined task [53]. The classification of UAVs is presented in Figure 5.

The oceans cover two-thirds of Earth's planet, but it remains a very poorly explored and vaguely understood dominion to date. The currently existing tools, techniques, and equipment available to explore this mysteriously hostile environment are limited. Given the scientific and commercial significance that the oceans offer, the UAV provides a valuable and feasible road to explore, exploit and conquer this otherwise challenging territory. These underwater vehicles are referred to as a marvel of underwater robotic technology. In recent times, AUVs are progressing towards becoming pervasive tools for oceanography and sampling. The AUVs are programmable, automatic vehicles widely variated in their physical design, making it possible for them to exercise various movements, such as drift, drive or glide through oceans with or without being manned by a staff or crew [54], [55]. The degree of control varies from task to task. So does the communication, which ranges from periodic to continuous, through satellite signals or undersea acoustic beacons.

A. APPLICATIONS

The functionality of AUVs is manifold, allowing for the conduction of sophisticated experiments from the surface ship, while the AUV navigates on the surface or in ocean depths to collect the data. Equipped with programmed devices and intelligence algorithms, advanced AUVs can make their inferences, adapt or adjust mission profile impetus the environmental data received over sensors in the course of the mission/experiment. Tasks range from simple measurement of water's physical characteristics, including temperature measurement, salinity analysis, monitoring dissolved oxygen levels, chlorophyll from aquatic microalgae, and estimation of the concentration of many fine particles. To perform sophisticated experiments, which may involve mapping the ocean floor, collecting images, sending them to a base station, and progressing through the ocean floor according to pre-determined directions [56].

Some of the economically useful facilities for a nation, such as hydropower plants, offshore platforms, oil and gas exploration/distillation units, depending on the quantities of these natural resources such as hydrocarbons, oils, and minerals. These resources, in most cases, being a deep treasure underwater, require efficient and effective technologies for underwater exploration and exploitation, making AUVs almost inevitable. As a result, the effectiveness of AUVs in oceanographic surveys, bathymetric measurements, and underwater maintenance tasks has been established. Amidst growing concerns around the environment, global warming has emerged as a problem needing immediate attention. The adverse effects being expanding deserts and rising water levels. The AUVs are the best choice for conducting surveys related to global warming and environmental

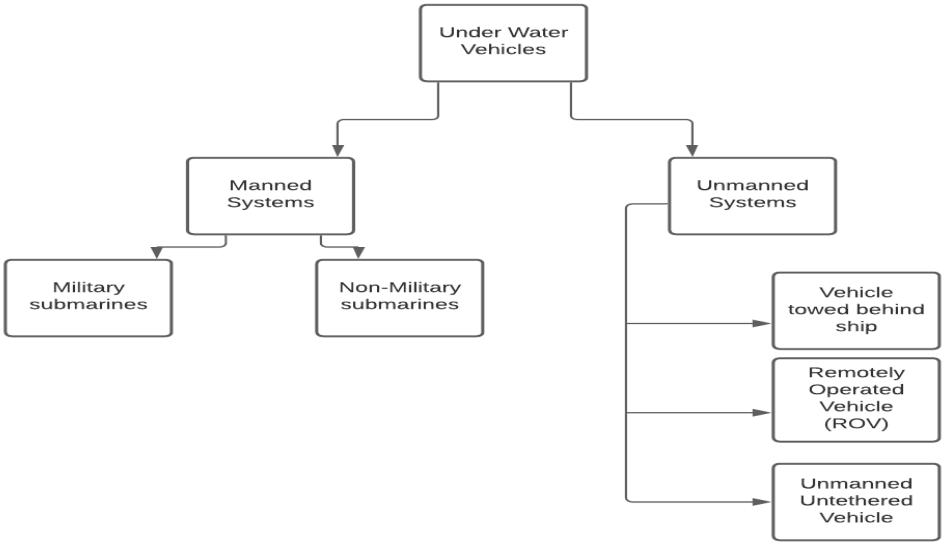


FIGURE 5. Classification of underwater vehicles.

problems. Specifically, in hostile and dangerous environments, the application of AUVs becomes all the more useful. For instance, they collect data deep in the oceans under dense layers of ice during the winter period. Compared to ROVs or towed vehicles, AUVs serve as a low-cost exploration solution and offer better quality outcomes during sensitive missions. AUVs are provisioned to sample water columns at oceanic depths, far beyond the human visit. Another vital application is underwater surveillance, which controls and monitors a given area to identify potential threats and perform tasks such as homeland defense, anti-terrorism, and safe disposal of explosives (termed, 'Explosive Ordnance Disposal') [54]. These underwater robotic missions are carried out prudently, ranging from identifying threats to their classification to the multitude of activities for anti-intrusion.

B. RESEARCH PERSPECTIVES AND DEVELOPMENTS

In several aspects, research activities are underway, furthering the applications of AUVs to make them increasingly effective. One of the key scientific challenges is enhancing the autonomy and the building team capabilities within underwater robotic vehicles to facilitate team/swarm missions. It is a vast area of scientific study and investigation, opening up avenues for future work in different application contexts. For specific underwater tasks, which cover reasonably large regions, it becomes requisite to have several robotic vehicles working together while collecting data samples from assigned sites and building inferences to take collective/individual actions. Thus, it requires building interoperability capabilities amongst the underwater vehicles and opens up several challenges related to building networking capabilities, communication protocols, distributed design, and communicating interfaces [54]. There are severe limitations in terms of limited bandwidth availability and latency issues involved in acoustic underwater messaging. IoT has emerged as a vital area, bringing together various things/items with sensors installed within an environment. The sensors act as input points receiving data from the environment. The data inputs are used within the system to facilitate the desired action concerning the pre-planned task. The advent of IoT has transformed several otherwise conventional devices. Over the years, IOT research has evolved and has been increasingly focused on building intelligent and autonomous systems.

The amalgamation of AUV and IoT is an area that has witnessed several novel developments and has been strongly progressing in recent times. While several intelligent devices have been developed over the years, securing data, ensuring reliability remains an ever-existing challenge, calling for needful attention. As vital decisions are expected from the intelligent devices and systems, strong emphasis is laid on their information source to ensure it is tamper-proof and secure. Disruptive technologies of the present generation, big data, and cloud computing are leveraged by IoT, and blockchain technology is next [57]. Blockchain is an emerging technology, revolutionizing and transforming how information is shared and accessed. Considering that underwater robotics involves AVs spread across distributed environments, interconnecting amongst themselves, and working together on sophisticated missions, it becomes essential for integration with blockchain technology to ensure trust in data transfer without authorities' involvement. Several case studies in the literature systematically prove how blockchain has demonstrated potential in improving existing IoT systems, be it in any application area.

Recent years have seen an advent in connected vehicles. Increasing demand for online booking cab services has brought a massive surge in these vehicles' design, development, and commissioning. It has incepted a concept of CVaaS, whose implementation is underway and progressing successfully. Exponential growth is witnessed in current times in V2V communication in vehicular networks. Thus, it has presented new requirements, such as safe, secure,

fast, continuous, and robust information sharing or exchange among vehicles within the connected vehicular networks. The original concept of vehicular networks has transformed into connected AVs. In this context, in AVs, congestion is reduced by allowing for access to current information by the vehicle instantly and promoting a better user experience. However, there are several issues related to security on the internet of vehicles. The malicious attacks may lead intruders to execute unethical acts, leading to the compromise of intelligent devices. Given the risk, blockchain technology is seen as a rescue, and it serves as the best technique providing secrecy and control system protection in real-time conditions. Addressing security need through a robust blockchain framework enables protecting the compromise of smart sensors of connected vehicles from the hacks of expert intruders. The blockchain framework functions through a systematic mechanism based on validating different security criteria such as identification of fake user requests, probabilistic authentication scenarios, and comparing with the intelligent device compromise criteria. Similar tools are underway for UAVs [58].

The decentralized blockchain-based mechanism is implemented in AVs to facilitate secure and reliable access to real-time availability information to ease the customers who may want to take a ride. Along the same lines, AUVs are also provided with advanced control systems and sensors to detect issues in the given environment, such as design faults leading to unsafe and civilian negligence. The blockchain serves as a decentralized tamper-proof business protocol facilitating a transparent, immutable, fast, reliable, secure, and cost-effective solution. The validation in blockchain protocols is through specifically designed consensus mechanisms. Abubaker *et al.* [59] proposed a proof of work consensus algorithm for verifying and validating the DR events in the network using the ethereum environment. Here, the 'Demand' ('D') is for the AV service, and 'Response' ('R') is the provisioning of the same. AV's design supports real-time traffic monitoring and rides supervision as AV accomplishes the desired task. With blockchain, the necessity for a banking institution or any trusted authority in between is removed, as it allows for secure provisioning service to end-user through the P2P mechanism-based vehicle sharing [59].

IoUT is a significant network of things for underwater scientific mission accomplishments, monitoring, and surveillance [60]. Connected AUVs provide support to IoUT in terms of saving energy while communicating with remote base stations. While the distributed design of connected AUVs is highly advantageous and suitable to underwater operations, it presents several vulnerabilities that unauthorized users can exploit for unethical practices. Communication from remote areas between IoUT and UAV is a possible site for cyber threats. Blockchain offers a solution here, providing support through data security and integrity. Islam and Shin [60] presented a blockchain-based secure scheme with UAV integrated with MEC assisting underwater monitoring [60]. This scheme proves the existing facilities with a 5G-based MEC environment, reducing the error and improving performance.

V. ARCHITECTURES AND INFRASTRUCTURE FOR UAV

This section discusses various requirements associated with UAV and their functional architecture. This explicit content presents the background knowledge for a better understanding of the integration of blockchain in AUV design. Understanding design aspects is helpful to comprehend the process used to store and process IoUT data securely, handle trust issues, ensure transparency, security, and immutability while customizing blockchain integration. Details are presented as follows.

AUV Design and Design Considerations: AUVs are complex units that involve several components, interconnected physically and working together functionally towards a goal and accomplishing a pre-defined task. The structure is difficult, and the design and development pose copious challenges of varied nature ranging from waterproofing, static and hydrodynamic stability and security, propulsion, power consumption, storage and waste minimization, monitor and control, and navigation. This is a quiet vibrant field of research and presents a cross-section of disciplines intersecting with each other. Each of AUVs can be seen as a marvel developed with the coming together of disciplines, mechanical, electrical, and software (e.g., Vidyut). Apart from physical design, which involves concepts of electromagnetics and pneumatics, there is a hoard of soft technologies involved in giving AUVs their context-specific functionalities. Thus, there are technologies like image processing, robotics, AI, ML, remote communication, and embedded systems [61]. An AUV is not required to be knotted to a support vessel through a tether cable. Therefore, while designing them, the following are some of the significant design considerations: The environment, which could be seawater and there would be issues concerning water pressure, sink, in-availability of gas or battery charge stations, the possibility of usage of Global Positioning System and Radio Waves [62]. A typical design of an AUV comprises multiple onboard CPUs, a collection of redundant input units, which are mission-specific sensors, effectors/actuators, onboard power source, and a robotic manipulator for expert performance underwater. For autonomy and intelligence, an onboard advanced control software architecture is available that is programmed specifically to the intervention mission. It has a collection of specific sensors and effectors. Kim and Yuh [63] presented a review of AUV control architectures and presented a specialized architecture christened as SDBCA. The data acquisition speed of the sensors is low. The sensor data bus facilitates quick response from the control architecture. It increases the flexibility of system design. It is a hierarchical architecture and offers enhanced control and stable performance [63].

An AUV is a complex unit that involves several scientific and engineering disciplines and requires different

infrastructural facilities for its desired operation in a given mission context. NSTL elaborated that various technologies provide AUVs with their desired functionality, which may vary, case-to-case and as per the mission in question. These technology categories are Platform technologies, Enabling technologies, and Operational technologies. The Platform technologies primarily comprise the aspects dependent on the platform that the AUV is expected to function in. These constitute the phenomena related to hydrodynamics, control guidance and navigation, propulsion, power source, and hull-structure, to mention a few significant ones. The Enabling technologies provide the necessary facilitation and support for the AUV to function in its environment; some are concepts related to Vehicle Autonomy and Path Planning, Communications and Networking, Buoyancy Engine, AI, Expert Systems, Sensors, and Sensor fusion, and Recovery Aid. The category of Operational technologies comprises the day-to-day activities involving a mundane/procedural/ operational context instead. These are concerned with payload systems (specific to payload sensors, payload release mechanisms, payload manipulators), Vehicle tracking, Launch and recovery, AUV launch control system, and game simulation for scenario studies [64]. The infrastructural facilities required for a typical AUV are mothership systems, docking systems, test and trail range, pressure test facilities, simulation platforms, and vehicle handling devices.

The early twenty-first century saw a surge in commercial activities successfully executed with AUVs, where AUVs moved into the commercial mainstream of the ocean industry. Design, modeling, identification, and control of AUVs are active subareas of research and development. Implementation of mechanical and electrical systems and integration of subsystems form the backbone of the consequences. Sensor and communication systems are the significant upper layer of products, another exciting development area for a typical AUV [65]. Several technology advances addressed in past decades are under the following aspects: Autonomy, Energy Systems and Management, Navigation, Sensors, Sensor Systems & Processing, 3D Imaging, Communications, Cooperative Systems, and Intelligent Systems. Quite a few of these have remained, 'Technology Long Poles' indicating that there is much to be accomplished in these, to have next-generation smart AUVs [53].

AUV Vision: The visual systems mounted on AUVs are responsible for capturing images, but this becomes a challenge in real-time environments with poor visibility. The robotic vision-based tasks capture images, but the quality in these extreme visibility conditions in real-time environments is poor, tends to be blurred, and is color depleted. Several computer vision techniques have been experimented with to render images, adapt the color space, and facilitate identifying features of interest. Robust control is used to ensure the stability of AUV at all times. For example, Pérez-Alcocer *et al.* [66] presented validation of their visual navigation system in real-time environments and discussed the feasibility of their approach.

Mission Characteristics in AUV Design: AUV design is specific for specific missions. It is to cater to the particular set of goals and associated requirements of the pre-defined task. However, some design considerations are common in all underwater environments, such as hydrodynamic drag, power, propulsion, maneuvering, and buoyancy control. Most significant here is the breath, as it affects the strength, transmission range, and endurance. The goal of underwater vehicles is to reduce drag, and it is a critical challenge in maritime hydrodynamics. This is achieved by experimenting with some of the following design considerations: shaping the hull in a streamlined manner, predefining and controlling boundary layer, timely polymer injection (can be replaced with slot suction), propulsion with focus on energy saving, through use of wake adapted propeller (also called as a suction slot with a stern jet), and appropriately controlled maneuvering for hydrodynamic stability. It controls the boundary layer and shaping of the hull, help in reducing skin friction and pressure drag.

Further, the propulsion helps the extraction of energy lost to fluid around the vehicle [67]. Design is an intricate concept, and AUV designers need to deeply study the physical and functional parameters and gain reasonable familiarity with the mission specifications. It is considering a prominent case of network design presented by Imad Jawhar and coworkers [68] that depicts the usage of LSN to assess the condition of the pipelines. Further, the AUV is programmed to follow the path along the channel, collecting data from the SNS. The collected data is delivered to the surface sink at the end of the LSN segment, which in turn, using WiMAX/cellular/satellite communication technologies, transmits it to the NCC. The design here allows for the flexibility to plan the placement of sensors and interchange between different AUV movement strategies. The overall advantages are quantified in reduced interference, collisions, terminal problems, and energy savings. A systematic procedure of measuring packet delivery ratio and end-to-end delay is employed to manage and iteratively improve network performance [68]. As specified earlier, the design of AUVs is a multi-disciplinary task. For instance, the aspects of guidance, navigation, and control theory/law, involve knowledge of different concepts, such as kinematics, dynamics, and hydrodynamics. The underwater environment is complex, and several issues affect the control design, such as hydrodynamic forces, which are non-linear and cross-coupled, that affect body elements of the vehicle, mechanical interaction with surrounding structures, disturbances caused to sensing systems/mechanisms, and GPS based orientation systems, due to attenuation of electromagnetic waves, issues caused due to ill-recording/noise/dropping-out of signals, the latency of sonar systems, poor visibility leading to limited vision and poor quality. The design of AUV is responsible for its specialized capabilities. For instance, Vidyut, a small-sized AUV designed at Sri Sairam Institute of Technology, has a non-conventional single-hull heavy bottom hydrodynamic design and has thrusters, six in number, allowing six degrees of the

freedom movement, enabling its motion control, that is useful in the identification of objects, and avoiding the obstacles that may be encountered, during its course. The Arduino Uno controller facilitates the maintenance of cruising and depth control [61].

AUV Size: The size of the AUV is an essential factor, precisely like the mission. Considering a problem setup, in the present case, of a fish infrastructure [69]. This is comprised of fish-cage nets that involve small-sized AUVs that are operational. This serves as a low-cost solution, allowing for frequent, efficient, and timely inspection, coupled with quick and prompt alarming services. Chalkiadakis *et al.* [69] presented an AUV architecture and supplementary analysis of operational characteristics in the context of design. The specifically designed architecture facilitates regular and periodic inspection, alerting information of net holes, faulty fittings, detection of fish-net functionalities by carefully navigating the aquaculture installation. The primary value of this architecture is the provision to provide an instant operative solution through a guide to corrective measures, elimination of fish escapes, and overall low maintenance/repair costs. The novelty of this architecture is a sophisticated design employing different sensors and advanced optical recognition techniques [69].

Sensors and Sensing Systems have progressed over time as imperative entities supporting capturing of data of interest. AUVs are a platform onto which the sensors and sensing systems are mounted [53]. The applications of AUVs are several, many of which necessitating contact of physical nature with the undersea environment, such as construction and repair, cable streaming, mine hunting, ammunition/weaponries retrieval, scientific investigations, plug-in, and plug-out [63]. The need for physical contact also has an essential role in AUV design. The initial days of AUV development focused on reliability factors. Once reliability was achieved, the focus shifted on adding sensors to acquire oceanic data. The efforts were towards integrating existing sensors and sensor processing and then towards the unique constraints of the AUV.

Further, developments shifted to developing novel sensors based on the constraints imposed by AUV and its environment. Thus, the effect of small-sized, highly reliable, robust, low-power, intelligent sensors was observed [53]. Research directions over the century have been under two aspects: the investigation of enabling technologies, furthering the development of AUV systems, and efforts towards designing, fabricating, and evaluating the AUV systems, under varied operational conditions, as per the context.

AUV Control Design: One of the vibrant areas of research in AUVs is guidance and control. It covers several types of controls and control methods ranging from conventional linear and non-linear control methods to model-based predictive, data-based, and adaptive management. Certain controls are specific to the mission, and further, there are focus areas related to underwater manipulation, position, and altitude estimation. Research work in the recent past in the area of control design is significant. AUVs are designed to move freely underwater without the need for a cable for power supply or communication. For instance, high-performance controllers embedded within AUVs are vital to facilitate precise maneuvering, which is an absolute necessity in scientific surveys and sophisticated investigations. One of the examples is AUV, designed by JAMSTEC. Some of the acoustic observation devices that the AUV is equipped with are side-scan sonar, sub-bottom profiler, and multi-beam echo sounder [62]. These devices have specific requirements, including stable cruising maintaining depth/altitude, the flow of direction, and information about the survey line. Thus, an advanced control system is available—this system facilitating high-performance maneuverability as a primary requirement. The design of a high-performance controller is based on a precise and high success rate-based vehicle dynamics mathematical model. The AUV design vehicle model uses 6 degrees of freedom.

AUV Navigation Design: Considering another significant development area, the navigation of AUV, that is, the vehicle's functioning in autonomous navigation mode. A desired set of instructions is preset on a computing machine before its observations in the target environment. This is a cruising schedule marked with a specific procedure to be followed by the observation devices. Typically, as the name indicates, a support vessel vehicle is used for supporting, escorting/safeguarding the vehicle. It moves AUV to the designated site. The instructions are duly programmed in the vehicle to handle obstacles. The vehicle implements suitable avoidance mechanisms over its cruising course almost independently, without unnecessary communication with the support vessel. Particularly in the case of long-range cruising, acoustic transponders may be positioned for reference purposes. This is helpful for the vehicle to correct its position by corresponding with the transponders in case it is disturbed during the cruising course. Another mode of operation of AUVs is acoustic remote control mode. Thus, it contrasts with the autonomous navigation mode, as the support vessel moves along with the vehicle and regular communication during the operations. Though the cruising schedule is pre-set, similar to autonomous mode, the pre-set instructions can be adjusted and downlinked from the support vessel by acoustic telemetry. At every few second frequencies, the transfer of images and data from the camera device and side-scan sonar is uplinked from the vehicle through acoustic telemetry.

AUV Autonomy Design: In the initial days, the design and development of the first generation AUVs was not around the demand for high-level intelligent behavior. Most of the tasks of AUVs were the tasks assigned along with pre-programmed instructions. Thus, the significance of autonomy in AUVs was undermined. Commercial success and market demand led to an increase in sophistication of tasks expected of AUVs, leading to development along the lines of shaping AUVs as more intelligent systems, better capable of adapting to the environment they exist [53]. AUVs operate in autonomous platforms that have certain specific requirements when it

comes to functioning independently. Developments in control algorithms and computing domains fueled the advances in AUVs. Thus, progresses outside the AUV community triggered developments in the AUV community. The eighties observed the size of computers getting reduced/miniaturized, power and memory requirements highly optimized, and implementation of several control algorithms for autonomous platforms. With software complex systems developed, autonomy progressed and became commonplace in many day-to-day gadgets and appliances. This has tremendously lowered the developments in the AUV community over the years, and several PoC prototypes are developed.

Further, the testbeds are developed and used. Developments in the field of artificial vision were used in the design and development of AUVs. While many problems were systematically solved, many others require intense research efforts [53]. The underwater environment is complex, uncertain, and unpredictable. AUVs and mobile systems traveling in such environments present issues in identifying accurate dynamic models and require the investigation of new control solutions that provide robustness. Lapierre [70] proposed a diving-control design that uses adaptive and switching schemes. This design based on Lyapunov theory and backstepping techniques was assessed for providing required robustness through a set of experiments.

Autonomy remains a research area, ever needing higher progress than achieved so far. Thus, it can analyze acquired data autonomously, yielding results that can guide cruising and control decisions. Underwater communication is challenging, and acoustic communications are the most viable one for a systems designer to experiment with. It offers a relatively low error rate and a reasonable range over kilometers at a few kbps bit rate. Thus the investigations are carried out using other technologies such as laser communication at short range and radio frequency communication (which has the advantage of being a noise-free communication) for over more extensive ranges. Challenges exist in communication which is to be between the multiple underwater systems [53]. Autonomous manipulation is an important aspect of AUVs, but a clear understanding of the system's mission is essential to ease the work of the system designer. There have been efforts to standardize the advances in system design and sharing across the community that helps apply the learnings to new missions, based on their similarity to the existent missions. A case-based approach is employed here, and such reuse has brought positive results [53]. Experiments based on real-time mapping, navigation, and control focus on improving autonomy in AUVs basis the advancement in algorithms. Chronological developments are initiating with real-time visual SLAM, cooperative multi-vehicle navigation, to perception-driven management. Eustice and coauthors presented work done at PeRL, worked on the AUV platform: Ocean-Server Iver2, and it is modified using a test-bed as a novel multi-AUV SLAM. Reference to this research, several AUVs were upgraded with additional navigational facilities and benefited from SLAM experimentation [71]. Flexible, easily adaptable production robot control architecture- Huxley- was developed by Bluefin Robotics [72]. The architecture has a layered design where logical abstraction controls the prime functions and an interface to allow the layers for joint functionality with proper interactions. An interface also helps in the expansion of core capabilities. The flexibility facilitates autonomy for the AUV, modifying its behavior and allowing users to design innovative payloads that can use available data [72].

AUV Modularity Design: As AUVs are usually unmanned, personnel costs are saved, and the complete costing model is focused around the specific mission/sampling that is to be tasked to the AUV. Due to the issue of diverse payloads, there is a great demand to develop modular designs. These modular vehicles can be reconfigured as per the requirement, suiting to host several loads. For instance, AUVs were designed by MBARI engineers [56]. Due to a modular design, there is no requirement to modify the essential components such as propulsion, navigation, power, and control [56]. Another common place design consideration is Modularity [53]. The design of distributed control systems architecture of hardware and software is promoted. AUV designers and developers are increasingly adopting the 'plug & play' concept, popularly implemented in PCs.

Multiple AUV Assembles Design: Early eighties shifted focus towards multiple cooperating AUVs [53]. The AUVs working on data acquired that can be aggregated and processed, leading to comprehensive, holistic high-resolution data describing the desired elements of the process of interest. Other developmental activities are the development of higher resolution imaging systems, of both optical and acoustic, that, due to advances in processors, can obtain higher resolution images over longer and longer ranges [53].

A. CONTEMPORARY RESEARCH AND DIRECTIONS IN AUV DESIGN

This sub-section presents the various recent research directions observed in the literature [53], [73]–[82]. Details are explained as follows.

1) AI IN AUV DESIGN

Specifically, in life-threatening activities, such as minelaying, surveillance, monitoring, and response to enemy attack missions, pioneering research work in the domain of UUAV, is presented involving AI. AI interventions span several aspects, such as underwater communications, autonomous navigation, and swam technologies. Reference [73] Whitcomb [74] demonstrated the current state, future directions, and technical challenges in underwater robotics, emphasizing AI-driven underwater robots.

Expert Systems is a field of AI, where human knowledge is embedded within a computerized system like a human expert can apply intelligence to the current situations and take decisions. One specialized AUV successfully tested in the North Sea is widely acclaimed in literature [75]. Its complete system architecture embodies several technological features.

Acosta *et al.* presented this architecture along with design considerations, experimental results, and trails. The real-time expert system – EN4AUV - was developed that takes trajectory control decisions for an AUV. The mission intervention of the AUV is to track the pipeline in the seabed. Its functioning is arranged around scenarios, and it is included on the board of the AUV CPU. Based on several variables, it analyzes, and for different techniques, suggests the trajectories. The detailed study of architecture reveals the components - dynamic mission planner, sub-systems – control, guidance, and navigation. The active mission planner houses the most important element – the KBPP, which holds the knowledge base with scenario-wise trajectory decisions [75].

2) OPEN SOURCE IN AUV CONTROL DESIGN

The design of AUVs over the past years depends on the closed-source-based control platforms. However, it poses severe limitations in modularity and flexibility. Aristizábal *et al.* [76] reported a methodology of designing a control platform, based on open-source practice, for an underwater vehicle, a remotely operated vehicle, named 'Visor3'. The authors outlined the issues in underwater systems concerning their interoperability and flexibility in interacting with other underwater vehicles and proposed novel system architecture with hardware, firmware, software, and control architectures. They presented a modular approach formed by interconnections of several frameworks, facilitating step-by-step, functional expansion, building up the whole solution. Overall, saving through an open-source system is in repair and fault-diagnosis processes, owing to the built-in simplification.

3) EVALUATION OF AUV DESIGN

Testing of AUVs is difficult, expensive, and due to hazardous environments for which it may have been designed, it is ineffective to simulate. However, in the absence of appropriate testing and evaluation of control algorithms, it cannot be accepted for research or commercial purposes. However, it necessitates the development of virtualized testbed environments. Sensors and control interfaces are used to integrate control algorithms with test-beds to model a vehicle and its environment (closest to the real-time environment, with specific characteristics). Gracanin *et al.* [77] proposed their virtualized test-bed-based environment approach and presented results of successful testing efforts. Keen interest was witnessed, with several labs, one of them being Draper Labs, which have developed two large AUVs, and deputed them only for testing activities, and designated them as 'testbeds' for several oncoming navy programs. In current scenarios, the AUVs have grown out of testbeds to be commercially realized for specific missions tasked to accomplish defined objectives [53].

4) AUV DESIGN OPTIMIZATION

With increasing commercialization, the importance of cost reliability and robustness is rising, and the industry is optimizing the same, economically working the trade-offs about the missions. AUVs are preferred over manned vehicles for survey operations, as they are inexpensive. Further, success in terms of their commercial usage has resulted in several efforts to optimize AUV design. Alam *et al.* [78] presented an optimized framework for AUV design based on two algorithms, NSGA-II, and IDEA. The authors gave their framework and ability to determine optimum preliminary design for AUV with different user requirements.

5) CONTEMPORARY AUV ARCHITECTURES AND AUV ECOSYSTEM

RAUVI– A novel architecture has been developed under this research project, a combination of underwater vehicles and a robotic arm. It is an innovative scheme that allows for response and planned actions on both subsystems. The response (responding action) is executed through a low-level control layer. This layer is responsible for communication with robotic hardware. The MCS supervises the intervention mission at a high level. The arm, vehicle, and control modules use the mechanism of actions and events to communicate with MCS. The intervention mission is executed in a supervised manner, with all components working in fine coordination. Sensor data is stored in a centralized sensor database and is used, as per requirement, for the successful functioning of the complete unit [79]. Connecting different things, such as cars or underwater vehicles or drones or rovers, is beneficial for commercial missions and needs vital infrastructure such as software to operate the unit successfully and services such as charging outlets and testing stations. The network built by the DAV foundation is a successful demonstration of the same, along with support infrastructure [80]. As AUVs operate in the complex environment over long periods, seldom stop for regular maintenance, there are instances where faults in components, especially sensors, go undetected, leading to loss of data and the vehicle itself in some cases. Shumsky [80] presented a method based on AQLPR for fault detection in sensors of AUVs. The authors described this method in contrast with the conventional techniques far from accurately detecting the sensor faults.

AUV industry is no exception, and several industries face the challenge of being severely fragmented. Commercial use of AUVs and its growing demand across the globe underscores a need for a supportive ecosystem that can foster the availability of all necessary services for it promptly and securely to facilitate leveraging its benefits to the maximum extent. A stable and robust ecosystem is developed by interconnecting various services and concerned service providers in an interoperable manner, employing open standards. The DAV Network foundation addresses this need by developing a decentralized transportation network that leverages a P2P system, connecting different participants and providing built-in benefits. The various participants comprise the consumers, producers, businesses, software engineers, hardware manufacturers, maintenance service officials, insurance providers, and any type of arbitrator service providers. The network

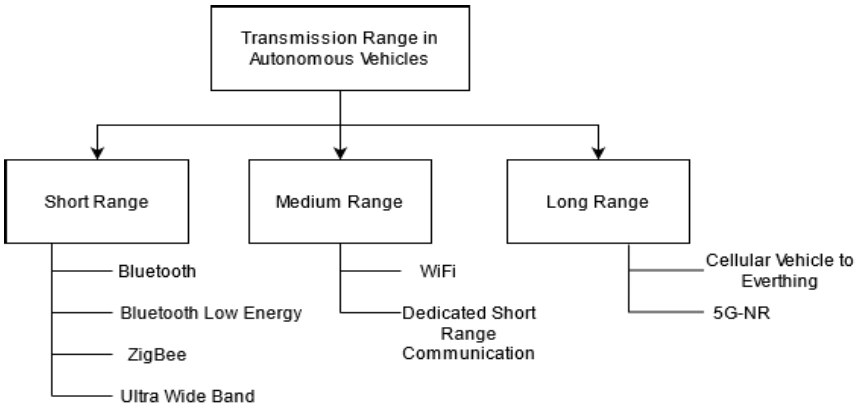


FIGURE 6. Transmission ranges in AVs.

is based on open-source protocols that are highly scalable and decentralized around options like communication and transactions. By open-sourcing the technology stack, the barriers to exchange and utilization of innovative solutions by participating entities are eliminated. In the AUV sector, the successes are restricted due to organizational issues and geographies, hindering their more comprehensive application. For instance, enabling AUVs and charging stations to communicate freely over the DAV network promotes commercial success, eliminating the barriers [81].

6) BLOCKCHAIN TECHNOLOGY IN AUV DESIGN

Table 4 shows a comparative analysis of recent studies over UAV [83]–[90]. The comparative analysis shows that very few studies and proposals are available for blockchain-based autonomous vehicle systems. The existing studies are theoretical discussions only. Thus, there is a broad scope to integrate blockchain technology with UAVs for ensuring transparency, security, and immutability. Handling trust issues and exchanging value in a secure and immutable manner is an important aspect. A wide array of applications belonging to various industries, built on top of blockchain technology, is a solution to handle it. DAV foundation applied the principle of P2P value exchange to the transfer of objects of interest, leveraging blockchain and smart contracts, allowing for secure transactions. Each participant vehicle or entity is assigned a unique ID on the network that facilitates tracking transactions and creates smart contracts on ID history. Communication in the network is in blockchain-on mode and block-chain-off mode. The smart-contracts signing, payments, and transactions happen in blockchain mode facilitating the leverage of benefits of blockchain technology. While the communication is to be carried out for finding an essential service such as a charging station or bay or maintenance workshop, the transmission is by AV sending a message for inviting bids and the stations responding. The AV chooses the best offer and proceeds accordingly. This communication is in blockchain-off mode.

Arbitrators and Insurance providers provide dispute resolution. The hardware and software providers assist in developing open-source platforms to ensure access to the network by all participants through a mechanism of DAV token [81]. Uddin *et al.* [82] presented a multilevel architecture built with sensor monitoring, consisting of layers of fog and cloud elements. These elements can store and process the IoUT data securely using customization options available with blockchain technology. The authors presented results of security and performance analysis over the architecture. After that, they demonstrated the method of routing IoUT data. The routing data is made possible by following the hierarchical topology, ensuring data validity.

VI. TARGET IDENTIFICATION AND TRACKING SCHEMES IN ON-ROAD AVs

In AVs, the vehicles collect information about their surroundings through various sensors, which facilitates driving the vehicles without the intervention of human beings. Hence, automation and networking are integrated into the autonomous vehicle. Thus, the sensors are classified as short, medium, and long-range [91]. As a result, the propagation ranges with different wireless technologies are depicted in Figure 6. The Short-range wireless technologies are used to establish communication over a distance of fewer than 25m while analyzing the essential characteristics such as data rate, power consumption, and transmission time. The medium transmission ranges from 25 to 100 meters and employs WLAN and DSRC technology to give excellent mobility. It allows operations to take place outside of a primary service set mode. The DSRC has a shorter latency of 100ms and permits communication without authentication. However, DSRC transmission range applications are limited to traffic and vehicle management.

Further, it suffers from serious security problems. The long-range transmission is from 100m to 5km. The cellular V2X is associated with third-generation technologies such as LTE and LTE-A. This technology provides a high rate, widespread coverage, and low to medium latency. As a result, it does not handle the safety-critical applications owing to the cellular traffic load, ranging in delay from 50 to 80ms [91]. Hence, this work focuses on short and long-range identification and tracking systems.

TABLE 4. Comparative analysis of recent studies over autonomous underwater vehicles.

Author	Year	A	B	C	D	E	F	G	H	I	J	K	Major Findings	Major Shortcomings and Challenges
Hu et al. [89]	2020	×	×	✓	✓	✓	×	✓	✓	✓	✓	×	In this work, a secure, and efficient scheme is proposed for an unreliable underwater environment using blockchain. This scheme is used for data collection, transmission and storage in an IoT underwater environment.	Blockchain-based solution is proposed to secure the IoT underwater environment. However, no proposal is made to evaluate the blockchain performance.
Gomes et al. [84]	2020	×	✓	×	×	×	×	×	✓	✓	✓	×	This work has prepared a survey of underwater object detection techniques in a comprehensive way.	This work is a survey work and no discussion over blockchain-integrated object detection is discussed or proposed.
Xu et al. [85]	2020	×	×	×	✓	×	×	×	×	✓	✓	×	This work is focus over event-triggered distributed adaptive bipartite consensus control algorithm. In this algorithm, multiple autonomous underwater vehicles are considered for consensus control using proposed algorithm.	Using proposed algorithm error in tracking is controlled and an example shows its effectiveness. However, no blockchain-based discussion is performed in this work.
Liang et al. [86]	2020	×	×	✓	✓	×	×	✓	✓	×	✓	×	Three-dimensional trajectory tracking for an autonomous underwater vehicle is discussed using fuzzy dynamics.	A mathematical and simulation-based experimentation is performed to prove the concept. However, no blockchain-based solution is proposed or integrated.
Bonin-Font and Burguera [90]	2020	×	×	✓	✓	×	×	×	×	✓	✓	×	This work presents a hash-based loop closure methodology for visual simultaneous localization and mapping (SLAM) in underwater autonomous vehicles. A conventional neural network-based experimentation is performed for image descriptor.	This is an experimental work with simulation and analysis using different datasets. However, no blockchain-based proposal is made or discussed in this work.
Wróbel and Weintrit [88]	2020	✓	×	×	×	×	×	✓	✓	×	✓	×	This work is more over theoretical discussions over how autonomous vessels and future hydrographers can be integrated to have mutual benefits.	This is a theoretical development and discussion work only. No blockchain-based solution is proposed or integrated.
Yin et al. [83]	2021	×	✓	×	✓	×	×	✓	✓	×	✓	×	This work is over recent studies on situation reasoning for autonomous underwater vehicles. The proposed situation reasoning is verified using simulation.	No proposal or association is made with any concept of blockchain. The framework is proposed and validated with simulation without any security concern.
Liu et al. [87]	2021	×	×	×	✓	×	×	×	×	×	✓	×	This work proposed a mechanism to guarantee frequency and time domain behaviour control. To control this, they used fractional-order proportional-integration controller.	A mathematical and simulation-based approach is followed to control the operations. No blockchain-based solution is proposed or integrated.

A: Short survey, B: Long and in-depth survey or analysis, C: Implementation-based study, D: Simulation-based study, E: Blockchain proposal discussions, F: Smart contract, G: Power/energy/charging-issues, H: Infrastructure Requirements, I: Application-level discussions, J: Autonomous Underwater Vehicle, K: Advanced technologies discussion (like IoT, Cloud, 5G, Industry 4.0, AI, ML and other).

TABLE 5. Comparison between exteroceptive sensors.

Sensor Type	Coverage Range	Pros	Cons
LiDAR	250m [93]	High reliability A dense network of the point clouds with high resolution	High cost and limited accessibility
RADAR	5 to 200m [94]	Low cost and increased accessibility Endures adverse weather conditions	False alarms are produces as a result of nearby metal artifacts Low-resolution images
Camera	250m [95]	Low cost and increased accessibility	The amount of computing power required for data analysis Susceptible to inadequate lighting Weather conditions are impacted
Ultrasonic	2m [95]	less expensive Endures adverse weather conditions	Because of the medium and ambient variations such as temperature and humidity, sound wave stimuli have a significant impact on sensors

Based on Table 5, the different sensors are used in the transmission ranges helps in mounting the communication in the V2V, V2I, and V2X [92]. Conversely, the AVs employ many types of sensors, such as exteroceptive and proprioceptive sensors. The exteroceptive sensors gather the data from the environment and measure the distance from the object. The proprioceptive sensors assess the values from the vehicles, including motor speed, wheel orientation, and joint angles. LiDAR, RADAR, camera, and ultrasonic sensors are an example of exteroceptive sensors. The camera sensors are passive light sensors: visible–light and infrared-based cameras. The LiDAR is the long-range sensor with 250m

[93], while RADAR is rated as short to medium with 5 to 200m [94]. The camera sensor range is approximately 250m. It depends on the lens efficiency, and the ultrasonic sensors have a range of 2m [95]. The proprioceptive sensors include GPS, the IMU, and the encoder. Hence, Table 5 presents a comparative analysis of the exteroceptive sensors along with their pros and cons. Figure 6 and Table 5 categorize the sensors and propagation ranges, the target identification, and tracking systems. Transmission ranges and association with AVs are explained as follows.

A. SHORT RANGE TARGET IDENTIFICATION AND TRACKING

The short-range target identification and tracking systems employ a series of sensors to identify targets such as a vehicle, malicious user, and road detection. Therefore, the existing schemes that encourage stability, reduce road collisions, increase energy efficiency, boost convenience and enhance vehicle performance are discussed with discussions as follows.

1) VEHICLE DETECTION

Vehicle identification schemes are classified into two types: appearance and motion-based strategies. An appearance-based approach helps to detect vehicles based on various characteristics such as color, texture, symmetry, headlights, and shadow effects. An optimum flow and complex background methods are used in a motion-based scheme. Additionally, the vehicle locations are extracted using ML techniques such as SVM and AdaBoost classifiers paired with Haar functionality. ML target tracking algorithms such as R-CNN, SPP-net, fast R-CNN, and many others have been used in the past few years. However, these approaches demand computation. As a result, neural network approaches such as YOLO, SSD, and YOLOv2 exist, which slowly increase processing speed but suffer from speed and accuracy trade-offs. Therefore, image-based short-ranging methods are employed for the stereo and monocular vision ranging. The stereo vision ranging extracts the target vehicle and computes the distance using 3D features [96]. However, since this approach employs many cameras, distance measurement involves a considerable amount of computation. The monocular vision ranging uses the bounding box to compute the distance.

Adamshuk *et al.* [97] employ the images' pixels, while Han *et al.* [98] employ the lane line, and Rezaei *et al.* [99] use the height and camera angle. These techniques, however, have no relative distance for the target and depend exclusively on the camera image. Hence, Zhao *et al.* [100] employed the vehicle plate detection method to analyze the space. Still, the range is restricted because of the long-distance and small plate size leading to inaccurate results. Zhao *et al.* [100] propose an optimized lightweight YOLO network with few parameters. This approach employs the license plate detection algorithm, which measures the distance based on vehicle width and computes the distance between vehicles. Further, a ranging fusion solution based on the two focal length cameras is designed to solve the small plate detection problem.

2) ROAD CURB DETECTION

Road curb detection is classified into structured and unstructured detection for AVs. The structured road detections depend on road divergences, hurdles, and corners. It is extensively focused on vision-based sensors and computer vision technologies. The identification of road curbs has primarily relied on vision-based cameras and machine vision technology. Therefore, vision-based road tracking algorithms rely on the algorithm rules rather than the datasets. Oniga *et al.* [101] propose stereovision sensors that collect the road curb segments using a rectangular area map with edge detection and Hough transformation schemes. Siegemund [102] identify the road curbs and surfaces using the conditional random field. Wang [103] employ the Naïve Bayes Framework that fuses the road curb points' various characteristics, hence offering a high certainty. As a result, these tactics are adequate for basic driving scenarios. However, the downside is, it is light-sensitive, subjective to adverse weather conditions, and offers unreliable distance information.

B. LONG-RANGE TARGET IDENTIFICATION AND TRACKING

The short-range target identification and tracking systems are effective under simple driving scenarios. However, these approaches are influenced by light and weather conditions. Thus, the information acquired through the short distance is intrinsically inaccurate. They are not robust enough for realistic problems. Consequently, the long rage target Identification and Tracking techniques are emerging.

1) ROAD CURB DETECTION

Kang *et al.* [104] suggest a 2D-LiDAR based road curb detection system that communicates with the multiple model framework. However, the sparse evidence does not correspond to the ambient experience. Hence the focus shifts to 3D-LiDAR point cloud data with 360-degree coverage. Peng [105] suggest a two-layer attribute extraction method that includes height jumping and slope, consisting of the false points and excluding surface points. Hu [106] extract the attributes dependent on boundary layer and elevation distance from obstacle points. Hence, these approaches generate the computing overhead. Wang [107] and Zai [108] extract the features based on super voxels, but they are not optimal for cloud points. Therefore, these approaches share common pitfalls such as single or multiple outliers that result in false detection. Yao *et al.* [109] propose a method to extract line segment features that suffer from cloud point distance. Wang *et al.* [110] offer a multi-feature flexible threshold approach for removing the cloud points from the density-based model. This model distinguishes between the left and right positions. Then, the false facts are filtered depending on whether they are inside and outside the lane. Lu *et al.* [111] suggested an unstructured road curb detection method using a 3D-LiDAR sensor. The road boundary detection algorithm extracts the spatial distance and angular

TABLE 6. Comparison between traditional and blockchain-based AV.

Security Parameter	Traditional AV	Blockchain-based AV
Failure	uses the central storage system hence single point of failure	uses the distributed storage system hence no single point of failure
Data Modification	data can be modified	Immutable
level of Data control	limited control over the data	High-level control over the data
Tractability	Medium	High
Accountability	Low	High
Fault tolerance	Low	High

features that remove cloud points above ground. The boundary point tracking approach is built on the Kalman filter, which forecasts and changes the boundary point information in real-time to avoid false and chaotic results.

The experiment results demonstrate that the proposed algorithm is capable of more accurately verifying the mined road data. It is possible to employ a variety of mobility tracking techniques focused on the single-vehicle and multi-vehicle multi-sensor. The single-vehicle multi-sensor approach achieves high precision by relying on onboard sensors such as GPS, IMU, LiDAR, and SLAM. However, incorporating these sensors in a single vehicle incurs high costs and sacrifices efficiency [112]. Therefore, there is a switch to the multi-vehicle multi-sensor that uses V2X to share the information with the neighboring vehicles. Hence it increases the localization and tracking performance. However, it faces various security challenges [113], [114].

Malicious participants, on the other side, gain a legitimate identity and enter the cooperative tracking network. Hence, a reputation-based approach, Data authentication, and secure localization approach are used to identify and track malicious users. Thus, the fast localization algorithm distinguishes the malicious users through the filtering and detecting algorithms. The filtering algorithm reduces the amount of false information from the network via the LMS [115], MMAE algorithm [116], [117]. MMSE, Attack-Resistant Minimum mean square estimation [118], CMMSE [119] are used as detection algorithms. Later detection algorithms that focus on hypothesis checking are used, such as the GLRT [120] and MNDA [121]. Hence, these algorithms are practical for static positioning but not for dynamic tracking. Therefore, Pi *et al.* [122] proposed a dynamic cooperative tracking algorithm that leverages the sequential similarity of mobility analysis to identify malicious users and false information. Therefore, the two sequential detection algorithms are used: DMMSD and MRED. Thus, the proposed data fusion and sharing paradigms are combined with the current tracking fusion algorithms to create a complete cooperative tracking scheme.

VII. SMART DATA HANDLING METHODOLOGIES FOR AVS USING BLOCKCHAIN

AVs communicate and share valuable information such as road conditions and traffic situations. This information is shared among the V2V and V2I over the internet. However, the data collected from the environment through the camera, RADAR, or LiDAR is stored in the cloud [123]. As a result, drivers or vehicle owners may benefit from this information. However, it creates privacy challenges such as tracking the drivers' location or analyzing their behavior. In addition, the Internet of Things employs sensors to connect vehicles to the Internet. Thus it helps to detect the drivers' diversion, tiredness, vehicle safety, and security problems solved through cloud technology but not wholly [124].

Moreover, the automotive industry is moving towards digitalization. Hence the illegal distribution of the vehicle data such as drivers, owners, passengers, and manufacturers' details is to be avoided [125]. Therefore, innovative solutions are required for data sharing in AV.

In AV, posit the blockchain technology to overcome the challenges that are under discussion. Blockchain is a distributed ledger that stores the time-stamped data. The vehicles participate in the distributed network and share the data in a reliable, privacy-preserving manner without using a trusted third party [126], [127]. Besides, blockchain maintains the user transactions securely, thus provides anonymity and uses the incentive mechanism. Hence, the comparison between traditional and blockchain for connected vehicle's security challenges is listed in table 6 [128]. Table 7 summarizes the adaption of the blockchain technology and security parameters for two vehicles that perform the various functionalities without any human interaction and by sensing the surrounding environment. Therefore, the blockchain-based methodologies are discussed with perspective to the categories of vehicles. Rowan *et al.* [129] proposed a secure inter-vehicle communication in the presence of the attack or compromise vehicle operations through side channels such as ultrasonic audio and visual light. This approach protects against attacks and verifies the location. The handshake protocol establishes secure communication by limiting the side channel flow to 176 bits. The data sharing between untrusted vehicles and manufacturers uses the physical side channels and blockchain infrastructure. The side channels provide the direction-based secure transmission between vehicles using symmetric encryption and message passing authentication keys. Barber [130] proposed a blockchain model for autonomous car communication and examined the benefits of blockchain technology, including data security, integrity,

TABLE 7. Summary of security challenges involved in categories of vehicles with blockchain.

S.No.	Author	Blockchain Type	Vehicle Category	Security and Privacy				
				Data security	Privacy	Transparency	Reliability	Human safety
1	Rowan et al. [129]	Public Blockchain	Autonomous Vehicles	√	X	X	X	X
2	Reid [130]	Public Blockchain	Autonomous Vehicles	√	X	X	X	X
3	Sananda et al. [131]	Consortium blockchain	Autonomous Vehicles	√	√	X	√	X
4	Alina et al. [139]	Private Blockchain	Autonomous Vehicles	√	X	X	√	√
5	Hao et al. [140]	Public Blockchain	Autonomous Vehicles	√	X	X	X	√
6	Chuka et al. [141]	Private Blockchain	Autonomous Vehicles	√	√	X	√	√
7	Hao et al. [142]	Private Blockchain	Autonomous Vehicles	√	√	√	X	X
8	Geetanjali et al. [143]	Private Blockchain	Autonomous Vehicles	√	√	√	X	√
9	Baza et al. [144]	Consortium blockchain	Autonomous Vehicles	√	X	X	X	X
10	LI et al. [145]	Private Blockchain	Autonomous Vehicles	√	√	√	X	√
11	Hong et al. [135]	Public Blockchain	Electric Vehicles	√	√	x	X	X
12	Zhou et al. [136]	Private Blockchain	Electric Vehicles	√	√	X	X	X
13	Song et al. [137]	Public Blockchain	Electric Vehicles	√	X	X	X	X
14	Xiaohong et al. [145]	Consortium blockchain	Electric Vehicles	√	√	X	X	X
15	Jiawen et al. [146]	Consortium blockchain	Electric Vehicles	√	√	X	X	X
16	Madhusudan et al. [132]	Public Blockchain	Intelligent Vehicle	√	X	X	√	X
17	Chuka et al. [133]	Private Blockchain	Intelligent Vehicle	√	X	X	√	X
18	Arushi et al. [134]	Public Blockchain	Intelligent Vehicle	√	X	X	√	X
19	Madhusudan et al. [138]	Public Blockchain	Intelligent Vehicle	√	X	X	√	√

Note: √ indicates the supports and X specifies the not supported

data availability, and privacy. Mitra *et al.* [131] designed the data and information-centric model for intra-AVs and assessed the security, tamper-resilience, and privacy through the use of the consortium blockchain. Singh and Kim [132], Oham *et al.* [133], Arora and Yadav [134] proposed an IV communication using blockchain technology. Thus, it introduces advanced technologies-based integrated environments to improve autonomous vehicle performance and reduce the chances of failure. Further, local and global optimum solutions are proposed to identify the best possible scenario for IV to operate. Singh and Kim [132] employs the 'trust bit' that enhances IVs privacy. The 'trust bit' allows IVs to communicate quickly and securely, and it stores the previous transactions and reputations of IVs communication in the cloud. Hence, the 'trust bit' can be accessed at any time. Oham *et al.* [133] propose a segmented distributed ledger framework for AV adjudication and auto insurance claims prohibiting unauthorized access to data that contributes to evidence. The evidence modification is caused by malicious actions from possible liable parties, which is prohibited through the dynamic validation protocol. Arora and Yadav [134] propose authentication and secure data transfer algorithms to include blockchain into the IoV. As a result, it employs smart contracts and PoW to ensure safe and secure data sharing between vehicles. Liu *et al.* [135] emphasize the security concerns in electric vehicle cloud edge computing, such as the energy and information exchange between electric vehicles. Electric vehicles play different roles based on the context-aware blockchain as data-coins and energy-coins recommended by distributed consensus algorithms. Through proof of work, the data frequency and energy contributions are applied. Su *et al.* [136] propose an energy-based private blockchain for safe EV charging in smart grids. This strategy makes use of the three algorithms: smart contracts DBFT and optimal contract. Electric vehicles are charged using smart contracts. A reputation-based DBFT consensus algorithm is proposed. After that, it uses the optimal contracts that satisfy the individual EVs' energy requirements to optimize the performance. Finally, it employs an energy allocation approach that restricts renewable energy for EVs. Therefore, the experimental results show that the proposed approach is more effective compared to the conventional approach. Hua *et al.* [137] use blockchain technologies to propose a shared platform for handling battery swapping and trust. The battery's details and operating history are permanently stored in the blockchain network. Thus, this approach provides fair digital currency transactions between EVs and battery stations and assesses the battery quality automatically through smart contracts. As a result, the system is built on the Ethereum blockchain, which depicts the

battery swapping and refueling-based blockchain that provides trust between EVs and charging stations. Singh and Kim [138] propose a reward-based IV data exchange scheme that uses blockchain technology with the PoD consensus algorithm to trust the IVs. As a result, the proposed architecture includes a seven-layer computational model to standardize the blockchain technology to provide trust for real-time traffic data. Buzachis *et al.* [139] proposed an AIM paradigm for recognizing human mistakes and AV decision-making for critical problems. The primary goal of the proposed scheme is to secure V2V and V2I connectivity. Hence, the proposed scheme implements the MA-AIM, which uses the blockchain to provide security at crossing points or junctions. The IMA is responsible for monitoring each vehicle's crossing points and controls via DA According to Guo *et al.* [140], when the AVs are involved in the accidents, the cases are registered for forensic purposes by leveraging the blockchain technology. This scheme relies on the confirmations of various authorities. If the number of certification signatures passes the threshold, then the verifier approves the vehicles and enables creating a new block of case records. In this process, the proof of event consensus algorithm employs based on multiple signature mechanisms. Hence, it offers tamperproof and verifiable incident tracking for self-driving vehicles. Oham *et al.* [141] propose a blockchain-based platform for AVs risk attribution model. This model extracts tampered proof of evidence from the different entities to assist the stakeholders in making decisions. A private blockchain is used to prohibit unauthorized parties from communicating with approved parties. Guo *et al.* [142] developed a PoE scheme based on a dynamic federation consensus algorithm. This consensus algorithm offers irrefutable accident forensics by delivering tamper-proof and verifiable incident data. The statistical and conceptualized model validates through the Hyperledger and fast leader election algorithm. Therefore, the proposed method more precisely produces and preserves event data in the blockchain.

Rathee *et al.* [143] employ blockchain technology to solve the various security challenges in connected vehicles. The proposed approach validates multiple security challenges, including authentication, fake requests, device compromise, and stored user-rating manipulation. Compared to the traditional system in terms of security problems, the simulation results demonstrate an accuracy of 86% in detecting malicious nodes within the prescribed period and overall performance of 79%. Baza *et al.* [144] employ the blockchain and smart contract that proposes a distributed firmware update scheme for AVs. The proposed strategy makes use of the consortium blockchain, which different AV manufacturers form. As a result, it guarantees the integrity and authenticity of firmware updates. However, firmware updates are shared using the zero-knowledge-proof protocol.

Further, the attribute-based encryption scheme is used to ensure that only the authorized AVs can download and use a new firmware update. Huang *et al.* [145] propose a hybrid EV charging system built on a consortium blockchain-based model that guarantees the protection and anonymity of electricity trading. The primary objective of this scheme is to optimize customer loyalty while reducing the costs regards the distinct factors, including charging and discharging locations, driving speed of EVs, and waiting time. Further, the improved NSGA is used, which improves the optimal model performance. The experimental results show that the proposed scheme significantly improves customer loyalty and cost from various perspectives. Kang *et al.* [146] offer a buyer-seller electricity exchange over the localized PHEVs in the smart grid. This system provides demand response by incentivizing the discharging of PHEVs to balance the local power grid in the owners' self-interest.

Nonetheless, transaction security and privacy are critical concerns addressed by the P2P electricity-trading framework with consortium blockchain (named PETCON). The PETCON exemplifies the operations of localized P2P electricity trading. Further, an iterative double auction process is used to solve electricity pricing and the volume of the exchanged electricity among the PHEV. The experimental results demonstrate the double auction mechanism improves the privacy protection of the PHEVs, transaction security, and privacy protection. Li *et al.* [147] propose a decentralized and location-based model to address data integrity, including privacy concerns in traffic management. The proposed scheme employs a private blockchain as well as a non-interactive ZKRP protocol. The conceptual model is developed with the help of the cryptographic libraries, including the Hyperledger Fabric framework and Hyperledger Ursa. The results show that the proposed scheme protects real-time traffic data accurately.

According to table 7, the security challenges associated with connected vehicle categories and blockchain are enlisted and compared. The existing approaches of the AVs promote data security but need improvement in other security challenges such as reliability, transparency, human safety, and privacy. However, in EV and IV, transparency is a critical problem since none of the existing approaches supports it, and these schemes are plagued with other security issues.

VIII. SMART CONTRACT DESIGN FOR AVs

Blockchain technology is often considered the most significant breakthrough since the Internet, with individuals, businesses, and even governments adopting it. Smart contracts are an attractive feature of blockchain technology. As global processes become more digital, smart contracts are gaining in popularity and getting easier to create. They provide an alternative to standard contracts, which are often inefficient and expensive. Smart contracts are now accessible to optimize a wide range of financial and business processes. They are, in essence, self-performing, self-enforced protocols governed by clear terms and conditions. Smart contracts represent an entirely new approach to contracts. Instead of two or more parties signing duplicate copies of a paper agreement, smart contracts use blockchain technology to ensure compliance. Thus it reduces costs and simplifies contract negotiations.

A smart contract uses executable program code running on top of the blockchain to enable and execute an agreement between untrusted parties without the involvement of a responsible third party. This code establishes the mechanism of the transaction and acts as the final arbiter of the terms. The contract's legible provisions are compiled into computer code that can operate on the network [148]–[150]. Following are the key features of blockchain-based smart contracts and their association with AVs.

- ***Accuracy*:** The predefined terms of smart contracts are immutable and verifiable before they are deployed to blockchain network nodes linked with AVs infrastructure. Once the condition is met, execution happens automatically. Thus, accuracy is guaranteed in the absence of human or other performance defects. Through transparent, accurate implementation, autonomous precise execution reduces biased operations and boosts performance.
- ***Exclusion of a trusted third party*:** Blockchain technology is compatible with decentralized nodes. The smart contract allows instructions to be self-executed under specified terms and conditions. These are necessary features to overcome the majority of the flaws with centralized apps. Decentralization eliminates single points of failure while maintaining service availability. In round trip requests, decentralization eliminates significant data usage and operational delays compared to centralized approaches.
- ***Autonomy*:** Once the blockchain system reaches the trigger stage, it will execute the state of the programs and the sequence of events. Trigger conditions can be defined in smart contracts with the approval of all blockchain network participants. Execution is automated and initiated by a P2P state without the involvement of a centralized third party. As a result of the operations being decentralized and not relying on centralized third parties, the availability of the service is ensured.
- ***Forge Resistance*:** The integrity of the distributed ledger is validated through digital signatures for each transaction and block. Forge resistance is an important differentiating feature that adds value to the blockchain. Transaction records and execution logic are cryptographically verified and persisted on the network.
- ***Transparency*:** An Additional significant advantage of blockchain-centered smart contracts is the transparency of transactions. All participants in the blockchain ecosystem have access to the blockchain immutable ledger and smart contract logic. Transparency is a distinctive property of blockchain that makes it profitable compared to centralized databases.

Smart contracts can potentially disrupt finance, real estate, retail supply chains, the auto industry, communications, and manufacturing by changing international industry and business operations. They increase the efficiency and speed with which business arrangements are made and provide complete transaction transparency. Other benefits include increased security because all actions are recorded and available for scanning. In addition, the autonomous vehicle can engage in two-way communication with its environment and manage trades on its own through blockchain-based smart contracts. Figure 7 shows that AVs can use smart contracts to identify certified riders and arrange transactions such as battery charge schedules, toll collection, insurance expirations, etc. [151], [152].

The deployment of smart contracts using blockchain technology has changed the landscape of the automotive sector as well. Smart contracts reduce the administrative costs associated with implementing such policies and ensure that the process is transparent and trusted by all stakeholders and regulatory organizations. AVs can store quantitative incident parameters such as date of insurance, amount of fuel used, vehicle mileage, location of power and toll stations, and driver identity on the blockchain (as shown in figure 8). Each vehicle maintains its node on a blockchain network, which records all transactions and actions. When the input terms of the smart contract change in a defined event such as a natural disaster, the claim process starts immediately. Many other event conditions, such as fuel discharge, car maintenance schedule, vehicle battery charge schedule, toll payment, and driver license verification/validation, are triggered automatically through smart contracts, as illustrated in figure 8.

IX. AEV

On-road accidents are increasing with an increase in the number of on-road vehicles. Thus, road vehicles arise various other issues include on-road congestions, massive fuel and energy consumption, and harmful emissions in the environment. It has been observed in recent studies that many such critically social and environmental issues can be resolved using AVs, driving, or systems [153]–[155]. A self-driving vehicle, robotic vehicle, and driverless vehicle is nothing but an AEV [156]. Cars, light motor vehicles, trucks, buses are self-driving vehicles, and they never required human drivers to drive and operate the vehicle safely with control. The latest autonomous vehicle design utilizes various sensors, smart devices, software, and hardware to drive, navigate monitor, and control vehicles. As per the global perspective of an autonomous electric vehicle, it has been observed that it is not operating in full strength. A partial form of automation in an electric vehicle is introduced in variations of self-automation rather than the conventional car's operation. Research, development, innovation, automation are the key points of the futuristic development of the automobile sector. Hence automobile manufacturers are more concentrated on autonomous electrical vehicles. As per the global perspectives, substantial financial investment with focused time is given for the entire development of AEV by leading automotive players in Germany, the US, the UK, and Japan. Few of the leading players are sanctioned the law of autonomous electric vehicle operation and its testing in the countries mentioned above. Indian automotive players are contributing 7.5% to the GDP, and it

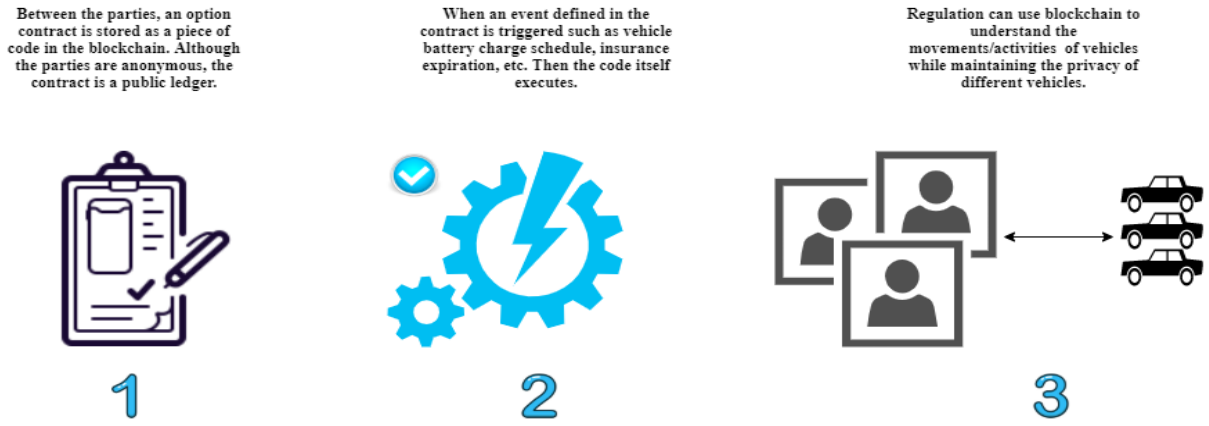


FIGURE 7. Life cycle of smart contract for AV.

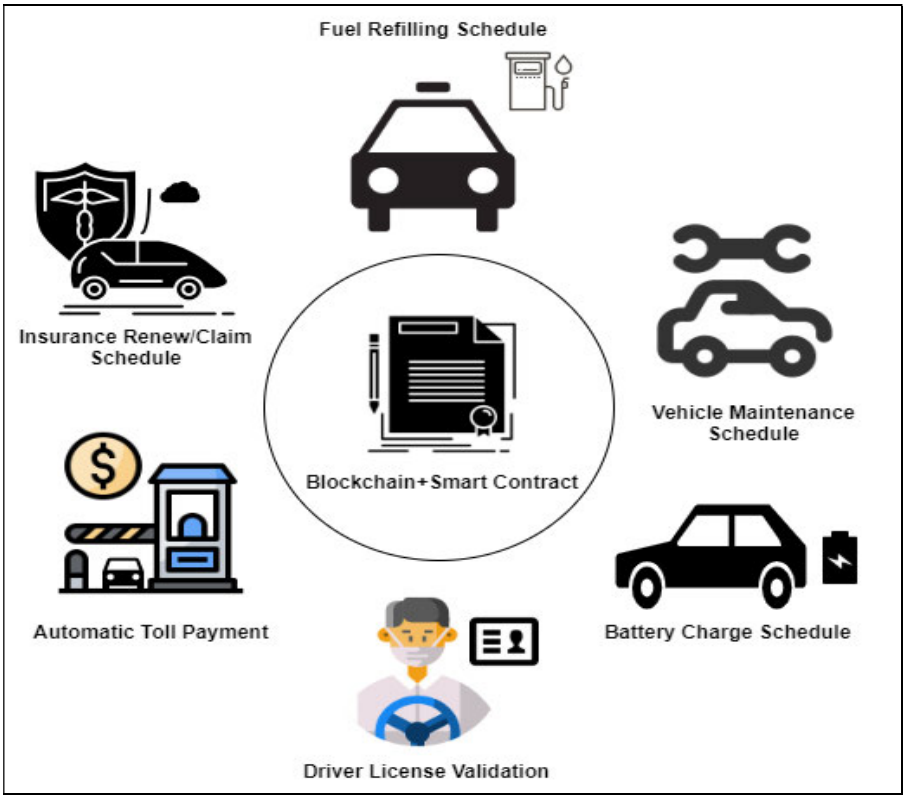


FIGURE 8. Execution of smart contracts for autonomous vehicles.

is the most significant contributor in the world's automotive sector.

The technology of AEV has overcome the problems of human limitations like inattention and tiredness. Figure 9 shows the classification of EV components and autonomous features. Further, the role of blockchain in this classification is explained. For example, they are developing a private, public, or consortium-based blockchain for electric vehicle body structure identification, sensing, or monitoring. Likewise, electric propulsion systems, energy sources, and auxiliary systems integrate sub-system blockchains to build the bridge blockchain. After that, easily ensure blockchain's various properties (immutability, transparency, enhanced security, distributed data availability, and faster transaction settlement). The following section explains the autonomous requirements.

A. TYPES OF AEVs

The utilization of driverless technology in AEV provides opportunities to overcome environmental, technical, and economic problems related to the transportation sector [157]. The existing nature of traditional transportation can be changing by using an autonomous electric vehicle to enhance safety in the transportation system by reducing human errors based on road accidents [158]. Transportation cost in AEVs is decreased due to the absence of human drivers. AEV

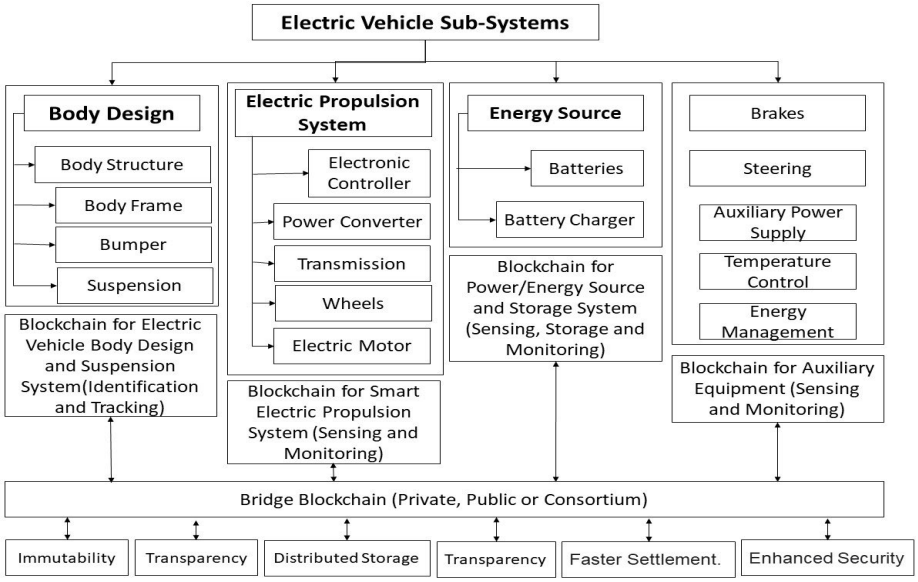


FIGURE 9. Blockchain and classification of electric vehicle sub-systems.

can be utilized for various applications like health check-up units, slipping units, and food units. The latest technological development and advancement of an autonomous electric vehicle have provided various smart city mobility opportunities [159]. As per the Automotive Engineers society [48], the following are the different types of AEVs.

1) **Type 1 (Zero Level Automation)**: In this type, manually operated vehicles are coming, and mostly this type of vehicle is available on the road. In this case, the human operator performs various driving tasks such as accelerating, braking, and steering. Hence automation level, in this case, is absent.
2) **Type 2 (Driving Assistance Automation):** In this case, the automation level is the lowest, and it will help the driving operator as an assistant for doing the operation of accelerating, steering during the cruise control. In the case of adaptive cruise control, the distance behind the car is safely maintained in this type 2 automation, and the driving operator is simultaneously focusing on other different tasks such as steering, acceleration, and braking. Controlling of the vehicle is obtained by a driving operator in association with automation as a driving assistant.
3) **Type 3 (Partial Automation):** In this case, the combination of automation tasks is employed, and under this situation, the entire monitoring of the surrounding environmental conditions and controlling of the driving activities are in the hand of the driving operator only.
4) **Type 4 (Automation with Condition, i.e., Conditional):** In this case, the human driving operator always is ready to handle the vehicle and operate accordingly at any time.
5) **Type 5 (High-level Automation):** In this case, the vehicle's operation is highly automated under certain offer conditions, and the driving operator may handle the vehicle operation under any circumstances.
6) **Type 6 (Complete Automation):** In this case, the vehicle's operation is completely automated under certain offer conditions, and the driving operator may handle the vehicle operation under any circumstances. In any situation, the vehicle is capable enough to operate under the self-driving mode of operation.

The detailed operational models of AEVs are mentioned in figure 10, which shows the various types of AEVs with different levels of operation. The above-detailed study finds that type 6, i.e., complete automation methodology for vehicle operation, is very flexible for transportation without drivers and feasible for goods and social transportation of various passenger pick-ups.

B. ENERGY EFFICIENT APPROACHES FOR AEVs

In the automotive sector, light motor vehicles are the most significant energy drainer at the global level. Autonomous electrical vehicles are a better alternative to existing fossil fuels or gasoline-based vehicles due to their merits. Improving the traffic conditions, reducing fuel requirements, and being eco-friendly are the salient features of AEVs. A flexible way of refueling vehicles is using fuel of renewable energy in an autonomous electric vehicle. Prototypes AVs can be used as fuel-efficient with drive programming. Reducing power consumption in an autonomous vehicle can be possible by taking programming-based activities such as GPS mapping in optimum route, speed, a distance of travel, and acceleration [160], [161]. In AVs, the adjustment of motion during the upcoming activities is saving energy by using automation. Energy efficiency in a specific group of vehicles increases due to cooperative driving and permitting the driving to proceed in a synchronized way. This energy-efficient movement

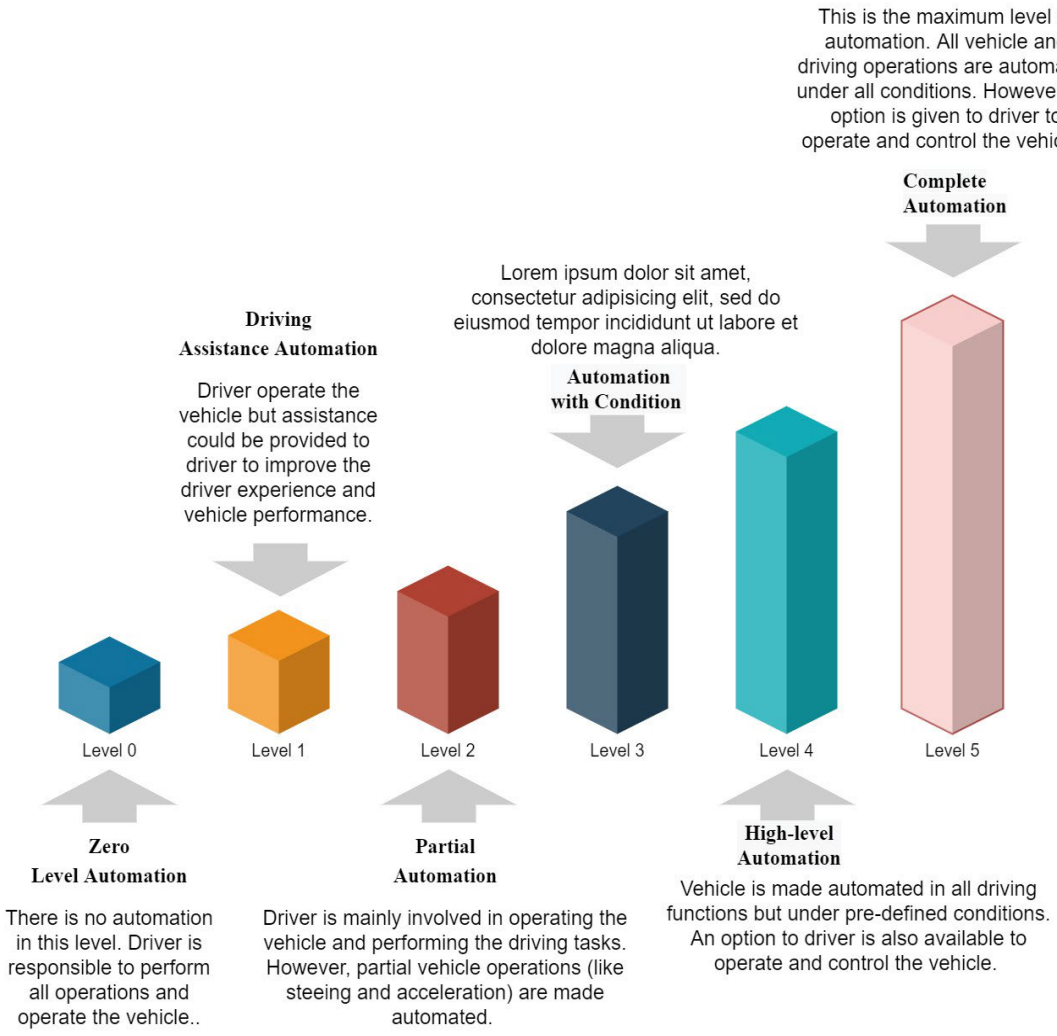


FIGURE 10. Detailed operational models of autonomous electric vehicle.

of an autonomous electric vehicle can help coordinate and exchange various effects such as mixed traffic for saving additional energy for nearby vehicles. By using prodigious access to different information with the help of advanced communication tools, novel sensors have enhanced the speed of processing the power with accurate controlling and positioning. Hence autonomous electric vehicles can be executed efficiently in the eco-driving mode of operation compared to the human-driving operator. Energy efficiency can be enhanced by selecting lanes for passenger cars following the coordinating vehicle [162].

C. METHODOLOGY OF ENERGY EFFICIENT APPROACHES

This section explores various technical research methodologies applied for energy-efficient approaches in electric vehicles. Details are presented as follows.

1) FUZZY LOGIC CONTROLLER IN AUTONOMOUS ELECTRIC VEHICLE

The fuzzy logic controller is used for speed control with the driver model controlling feature [163]. The criteria for control design with reduction of absolute internal error is considered, and its performance is compared with Fuzzy logic controller, i.e., type 1, PID of driver model control [163], [164]. Additionally, criteria of particle swarm optimization are involved in the control design. Similarly, the comparative analysis of consumption of energy in the autonomous electric vehicle drive cycle is considered. The fuzzy logic controller type 2 is saving energy in enormous strength with reduction of error.

2) AGENT-BASED TRAFFIC SIMULATION IN AUTONOMOUS ELECTRIC VEHICLE

In this autonomous vehicle case, agent-based traffic modeling and simulation systems are considered to provide good interaction between the utilization of autonomous vehicle benefits, executed via different control strategies, drive train, drive cycle modeling, and simulation [165].

3) OPTIMAL TRACKING SYSTEMS SYNTHESIS

In [166], the theoretical methodology of the optimal tracking synthesis system is proposed. Here, actual and desired outputs are compared and monitored. Further, the minimum error

between both results is noted while reducing energy consumption to its minimum [166], [167]. The vehicle's observations are planned to move from one location to another in association with algorithm design and development. Hence accordingly, follow the proposed track between the two locations, which is reflected in the specified map. The contribution of this approach is systematically remembered in the automation of electric vehicles [166].

4) SDN-BASED ENERGY EFFICIENT APPROACH USING INTERNET OF AVs

Due to technological development in AVs, the IoT is playing a significant role in forthcoming intelligent transportation systems. In this case, ICT is used to improve the operational activities of AVs and reduce energy consumption [168]. Due to the massive use of innovative technologies, smart sensors in AVs, a tremendous amount of data and necessary information need to be communicated with vehicles. Because of that, there is a need to enhance the connectivity between vehicles in the wireless mode of operation. Technical challenges arise during this data transmission because of traditional wireless communication systems such as communication system service, optimum utilization of resources, and network system. The powerful technology is employed to solve this puzzle through software-defined networking under the energy-efficient mode of operation.

5) CLOUD AIDED LEARNING SYSTEM: AN INITIATIVE OF ENERGY-EFFICIENT SYSTEM

During the operation of fast-changing conditions of AEVs, the necessary environmental information available in vehicles is not used optimistically in the propulsion system. Hence by initiating the efforts for understanding the environmental needs with a shorter span of distance, cloud-aided learning systems are used in association with the intelligent transportation system, GPS, intelligent cameras, RADAR system, and an ultrasonic system light-detecting and ranging. This entire combined system is developing the smart modeling-based system in the vehicle in a precise way for getting the information of the environment in a better way and reducing the vehicle energy consumption. In real-time vehicle operation, AI-based modeling techniques for environmental conditions update vehicles' propulsion systems. The energy-efficient and high-performance initiative of cloud-aided systems, cost-effective computational modeling, and optimistic operations are obtained [169].

D. SMART INFRASTRUCTURE FOR AEVs

External smart infrastructure is required for the effective operation of AEVs in association with the in-house physical components of vehicles. Following important internal physical components are used in an autonomous electric vehicle for conducting various activities.

i. During the driving of vehicles, various **cameras** are utilized for detecting the obstacles along with track roadway information and lane departure.
ii. Detection of short wave and long wave depth is done by using radio waveforms of the **RADAR** system.
iii. LiDAR is utilized with intelligent sensors for getting the 3D map of a particular area by illuminating the target using laser light.
iv. GPS is guiding vehicles for getting the correct position by using satellites.
v. The Ultrasonic sensors gather the information within kilometers, utilizing high-frequency sound waves and bringing it back to know the exact distance.
vi. The brain of the autonomous vehicle is a **central computer** that receives the communication information from various sub-components, and accordingly, the computer system guiding the overall operation of the entire vehicle.
vii. V2V communication is established by using a **DRSC** communicating device which allows the transmission of data in a wireless communication mode of operation in safer applications [170]

E. EXTERNAL SMART INFRASTRUCTURE

Proper external infrastructure is helpful for the fully automated operation of the vehicle. Due to the rapid industrialization in the automotive industry, there is a need for more innovative new infrastructure rather than the existing one, such as advanced lanes and telematics. Following are the changes to be adapted in the existing infrastructure for new AEVs [171], [172].

a) In the existing road, inferior markings are challenging for current vehicles, and hence there is a need to implement effective lane marking for AVs. The effective road marking should be machine-readable and appropriately reflective and is called a **smart lane marking system.**
b) The effective operation of AVs should involve smart roadside sensors on lanes and sidewalks, which permits a record of surrounding conditions and forthcoming dangerous conditions.
c) In existing vehicles, the road signs and symbols are to be recognized by the image recognizing system. Nowadays, intelligent AI-based machines are used for reading road signs automatically. AI-based devices use embedded coding for sign reading which can be transmitted and sends the necessary messages to the concerned users or drivers, i.e., Smart Signage.
d) Changing the cities and highway infrastructure is another important development in this area. The massive digital product, which is human-centric, makes the cities smarter for living by using the more innovative infrastructure. The AEVs traveling minimizes the crowding in a substantial populated area during traveling by AEVs and enhances road capacity. Due to the adaption of intelligent infrastructure, the look of the

city and highway changes, and no need for traffic signal lights shortly. The smart machine operates efficiently by deciding its priority while driving the vehicle.

e) Innovative parking facilities are also advanced. Identification of parking spots is complicated in a high-density city but using smart AVs is easy with the help of an intelligent infrastructure system. Narrow free spaces in the town are priory identified and notified to all. So that digital technology-based systems can quickly identify the parking for the concerned. So that the exiting allocated spaces for earlier vehicles parking can be used to enhance the intelligent infrastructure for vehicles.

f) Internet connectivity for vehicle infrastructure is improved. Utilizing AI technologies, ML, neural networks, intelligent sensors, and intelligent IoT appliances for driving AVs required massive internet connectivity with colossal speed. Thus, the network glitches are overcome through the latest 5G network through enormous data exchanges. So that smooth operation of the smart autonomous vehicle can be possible with the help of a 5G high-speed network without any interruptions. Infrastructure requirement for 5G network is different from that of 4G, hence installation of 5G based fiber optic cables throughout the way need to be executed. This new infrastructure will be helpful for the practical driving of AEVs. AVs can change the entire look of existing infrastructure and the optimistic enhancement of the public transportation system [172]–[174]. This exchange requires a high-speed internet facility which can be made possible easily using 5G or future generation networks.

g) Vehicle digital twin technology is changing the future. For testing electric vehicles, in-house infrastructure is required, which contains the equipment for measuring the on-road dynamic behavior of vehicles and chassis dynamometer testing set up by using vehicle digital twin's technology. Thus, the AVs perform the following tasks: modeling of vehicles, optimization of vehicles, virtual testing smart energy management system, and simulation in the virtual environment and analyze the facts.

F. BLOCKCHAIN FOR AEVs

Table 8 shows the comparative analysis of recent studies over AEVs [175]–[185]. Results show that few blockchain-based studies and proposals are currently available for AEVs. As discussed earlier, blockchain technology can give a wide range of advantages to autonomous systems. Thus, there is a need to explore blockchain technology and associated concepts for AEVs as well. Figure 11 shows a proposal for a blockchain technology-based automated electric vehicle system. Various sub-systems in this proposal are briefly discussed as follows.

- *Electric vehicle* system has five sub-systems, including charging, storage, data processing, power, and waste. All of these sub-systems can have their blockchain networks. More explanations about these sub-systems are discussed as follows.
- *Blockchain network for the autonomous electric system:* In AEV, all sub-systems have their blockchains interconnected to form a single blockchain network for AEV.
- *Blockchain bridge:* If there are multiple blockchain networks (i.e., each subsystem has its blockchain networks), the blockchain bridge helps connect and transfer tokens from one chain to another.
- *Blockchain network for charging:* A blockchain network for charging can have secure data transfer. This data includes the power sources information, distribution status, and power requirements.
- *Blockchain network for electric vehicles and power storage:* Each autonomous electric vehicle system needs information about its vehicle. For example, information about the electricity balance can help estimate how much a vehicle can travel.
- *Blockchain network for drivers:* Information about drivers, their wallets, and preferred payment gateways can be made available to blockchain networks private to drivers.
- *Blockchain networks for data processing units:* A cloud-based infrastructure for AEVs can provide advantages like information about vehicle location, movements, speed, charging requirements, and many more. Further, the blockchain-based network for data processing can build more trust in the system.
- *Blockchain network for power units:* This is the vehicle's internal performance parameter. This sub-system helps collect the power-related information from the vehicle and transfer it to other systems to fulfill future requirements. Integrating a blockchain network with this system can allow for secure measuring and sharing of the vehicle power consumption requirements.
- *Blockchain network for power waste management:* Power waster is another important parameter for the autonomous electric system. This parameter can help in estimating the vehicle condition and necessary service requirements. Blockchain can help in securely sharing this information with other systems (like insurance or maintenance and service provider).
- *Smart contracts:* Every two sub-systems in the autonomous electric system execute their operation using smart contracts. Smart contracts help in automated charge deduction based on vehicle' operations or activities.

G. CHALLENGES AND RESEARCH DIRECTIONS FOR AEVs

The autonomous electric vehicle is an intelligent vehicle operating using energy produced by the electric medium. This vehicle can run without a human driver operator by correctly sensing the surrounding environment. Further, it identifies the same on-road objects according to various pre-defined categories classified. It detects the navigation path according

TABLE 8. Comparative analysis of recent studies over autonomous electric vehicles.

Author	Year	A	B	C	D	E	F	G	H	I	J	K	L	Major Findings	Major Shortcomings and Challenges
Alkheir et al. [175]	2018	✓	×	×	×	×	×	×	×	×	✓	✓	✓	This article focuses over connectivity services, automation levels, and different types of autonomous vehicles.	No in-depth findings are observed in this work. Findings are useful to take up for proposal, simulation or implementation.
Damaj et al. [176]	2021	×	✓	×	×	×	×	✓	✓	✓	✓	✓	✓	Performance and quality issues of electrical vehicles are highlighted. Taxonomies, and frameworks are proposed for better quality of experience.	Use-cases or case studies are required to be taken up. The existing work can be extended to incorporate its application to electrical vehicles automation.
Huang et al. [177]	2021	×	×	✓	✓	×	×	✓	×	✓	×	✓	×	This work proposes a blockchain-based market mechanism for electric vehicle charging station. Proposed model is verified using mathematical verification and simulation.	Autonomous approaches are not integrated or discussed for electric vehicles. Blockchain-issues are more related with energy market rather with vehicle's internal or external operation parameters.
Hasankhani et al. [178]	2021	×	✓	×	×	✓	✓	✓	✓	✓	✓	✓	✓	Blockchain applications to smart grids are explored. Blockchain-technology and other advanced technologies are also explored for smart grids.	This work has done in-depth survey. However, use-cases or case studies of blockchain-based smart grids can be included to identify the parameters that should be taken care in implementation.
Subramanian et al. [179]	2021	×	×	✓	×	✓	✓	✓	✓	✓	×	✓	✓	A hybrid blockchain-based proposal is made for pre-owned electric vehicle supply chain. Discussions over cloud based infrastructure is also proposed in this work.	Comparative study with existing work or evaluations and improvement in performance-based framework is not explored in-depth. This is more of an application rather than addressing the research challenges.
Gowda et al. [180]	2021	×	×	×	✓	✓	✓	✓	×	✓	×	✓	×	This work has proposed a assessment and tracking mechanism for battery degradation costs. Here, a mathematical model is proposed and formal analysis is done.	This work is more of a mathematical analysis rather than framework-based implementation. The real-aspects of proposed approach can only be observed in real-time electric vehicle implementation.
Jamil et al. [181]	2021	×	×	✓	×	✓	✓	✓	✓	✓	×	✓	✓	This work has proposed a blockchain-based strategy for fuel payment in smart cars. This is an automation because it incorporates no human interaction. Blockchain is used to ensure transparency, trust and privacy.	This work has discussed the use of electric vehicles briefly. No specifications are drawn for electric vehicle-based fuelling system. Although performance of blockchain network is analyzed but this work can be extended to include the performance analysis of charging system in electric vehicles.
Thukral et al. [182]	2021	×	×	✓	×	✓	✓	✓	×	✓	×	✓	×	In this work, author claimed to design a smart contract for secure crowdfunding in electric vehicle charging station. Smart contract is programmed and tested as well.	A short smart contract is designed for analysis. However, detailed infrastructure and electric vehicles' internal and external requirements are not studied in detailed. A comparative literature or performance analysis is missing.
Wan et al. [183]	2021	×	×	✓	×	✓	✓	✓	✓	✓	×	✓	×	This work has proposed a privacy preserving fair exchange scheme using blockchain. A mathematical and implementation-based analysis is performed for performance analysis.	This work is an in-depth analysis of blockchain-based solution in privacy preserving fair exchange for vehicle to grid system. However, this work does not address the autonomous electrical vehicle system or its associated features. Thus, this work can be extended towards autonomous systems.
Distefano et al. [184]	2021	×	✓	×	×	✓	✓	✓	✓	✓	×	×	×	Blockchain-based distributed ledger is used to implement vehicle-centric information systems. The proposed solution integrates multichain network and MongoDB technologies.	This work is a theoretical discussion and development. Here, a logical flow to integrate two approaches is proposed. This work can be extended to simulate or implement for autonomous systems and electric vehicles.
Shaikh et al. [185]	2021	✓	×	✓	×	×	×	✓	×	×	✓	×	✓	This work has proposed a three layer hierarchical charging system with wireless static and dynamic options. Here, IoT and cloud concepts are discussed to make it feasible.	In this work, there is no blockchain-based solution to improve the security or performance for autonomous electric vehicles. Thus, this work can be extended to enhance it for blockchain-based approach to ensure security.

A: Short survey, B: Long and in-depth survey or analysis, C: Implementation-based study, D: Simulation-based study, E: Blockchain proposal discussions, F: Smart contract, G: Power/energy/charging-issues, H: Infrastructure Requirements, I: application-level discussions, J: Autonomous Electric Vehicle, K: Normal Electrical Vehicle, L: advanced technologies discussion (like IoT, Cloud, 5G, Industry 4.0, AI, ML and other)

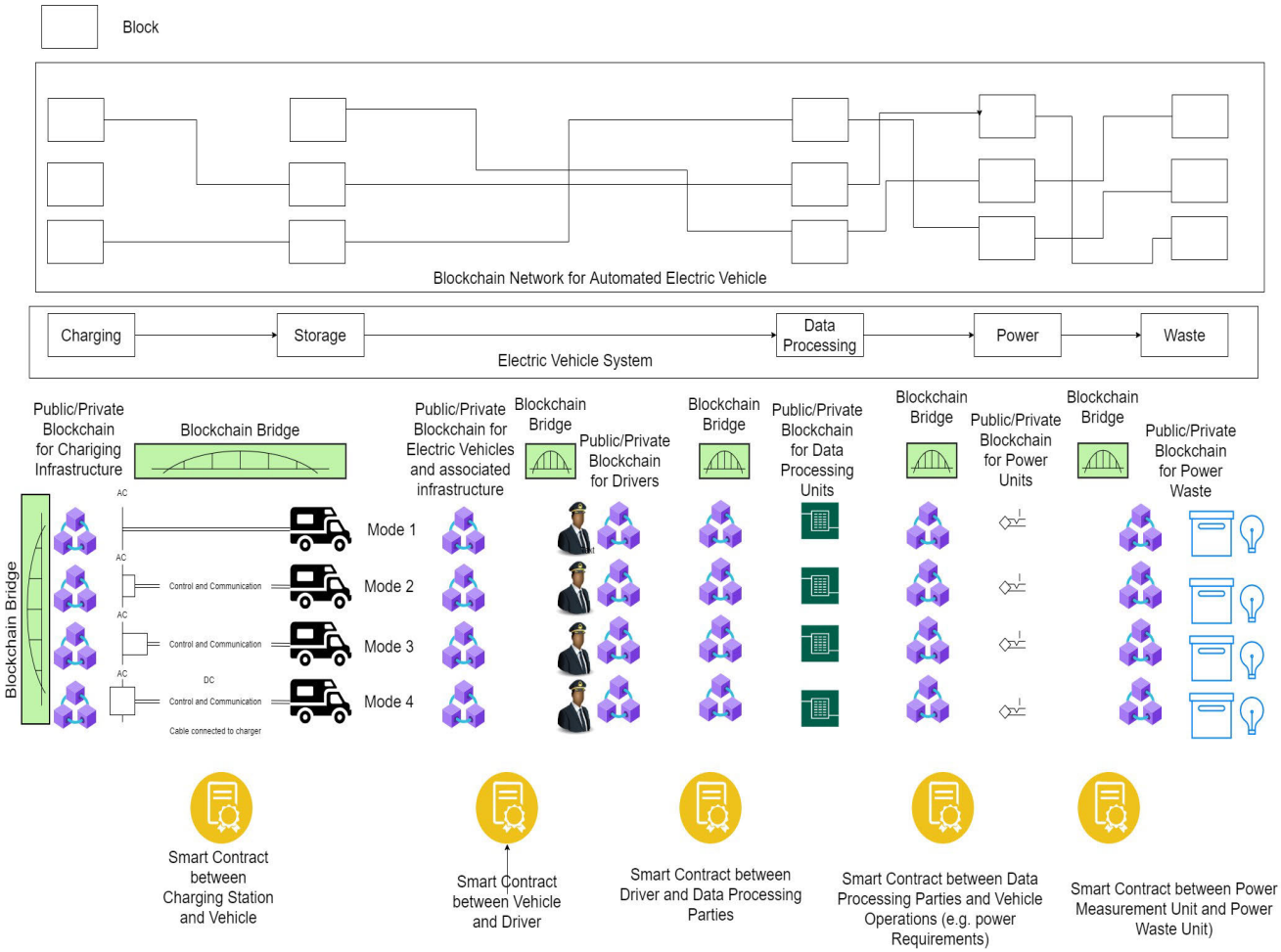


FIGURE 11. Blockchain technology and automated electric vehicle system.

to different information obtained from smart sensors and accordingly follows the transportation system rules and regulations during driving the vehicles [186]. AEVs create various questions about the security and safety of vehicles, principles, socio-economic aspects, and technological development before its execution on the road. Hence it is needful to understand the various challenges for the overall development of AEVs. Thus, it helps in designing multiple strategies for overcoming the challenges of vehicles which will help to enhance the overall performance of AEVs. The challenges and research directions are explained as follows.

1) CHALLENGES OF AEVs

This sub-section explains the challenges observed in recent AEVs [187]. Details are presented as follows.

a) **Sensors:** In AEVs, various smart sensors detect objects like traffic symbols, vehicles, signals, and road signs. Sensors can detect multiple objects and measure speed and distance under different environmental conditions. Information collected from various sensors is fused and transmitted to the computer or system that controls the vehicle and makes the necessary decision to either stop or steer. The accuracy of sensors is affected during bad weather conditions. Hence assurance is required that the implemented sensors can detect all the objects accurately from any location globally. Thus, it builds trust in the system and helps maintain safety throughout the vehicle journey [188].

b) **AI and ML:** Data collected from various sensors are processed using multiple AI and ML algorithms, which will help make decisions for taking particular actions. The acceptance of ML and AI algorithms are not matured globally due to safety constraints. Hence, there is a need to verify the safety aspects during the utilization of AI and ML in vehicle operations.

c) **Consumer's Acceptance:** As the technological development of AVs are in progress, but some of the particular factors that affect the acceptance of AVs are socioeconomic properties of the vehicle operator, population tally, operation and maintenance of vehicles, completeness abundance, and vehicle operator enjoyment. Hence there is a need to do more study on the area as mentioned earlier. Thus, enhancing the security of vehicles by changing futuristic technology [187]. As a result, customer acceptance improves.

d) **The Open Roads:** whenever AVs are running on the roads, updating infrastructure and upgrading is mandatory for vehicle performance enhancement. Vehicle running on new roads need to detect the objects accurately, and by changing the road conditions, it has to update its information via updates in software. From a safety point of view, previous and updated information needs to discriminate.
e) **Safety and Crashes:** The adaption of various safety appliances in AVs is appreciable includes forward-collision indication, antilock braking system, stability control system, airbag for protection of human life, and many others. Additionally, there is a need to add a lane departure indication system, the adaption of headlights to all vehicles uniformly, and physically handicap spot assistance. In this way, AVs can reduce the majority of crashes and also controlling heavy traffic delays.
f) **Regulations:** In any automotive industry, there are no standards, rules, rules for complete AEVs in present times. The existing measures are related to safety by considering the human operator to take control under emergency conditions. AVs have particular lane-keeping systems and policies as per the global standards, but rules and regulations incorporating advanced technologies (like AI, ML, and sensors) are not available. As a result, autonomous cars without proper rules and regulations are not safe for further operation.
g) **Social acceptability:** There is a need to address the public opinion about their decisions for accepting AEVs; otherwise, there may be chances of rejection of AEVs. The autonomous electric car manufacturer has to give evidence about safety. Further, it is complicated without public collaborations.
h) **Technological Development and innovations:** With new research tools and techniques in transportation systems, obtain the optimized performance in autonomous electric vehicles. Hence to do the same, there is a need to establish a robust structural framework and various methodologies [187].
i) **Blockchain technology:** This technology faces the challenges of lack of technical knowledge, i.e., how and what components of blockchain technology should be integrated with an autonomous system. Further, there is no experience handling blockchain technology combined with autonomous systems, especially the lack of hands-on training.
j) **Price of Autonomy:** The autonomous electric vehicle is made by various subsystems and intelligent technologies. The autonomous vehicle technologies are not yet matured in full strength. Hence, the cost of the vehicle varies based on the vehicle, and it is expensive compare to an ordinary vehicle.
k) **Increased Software Complexity:** With the use of advanced technologies and concepts (like sensors, cameras, controllers, AI, ML, and neural networks), the entire structure of the autonomous electric vehicle is complex. The complexity increases with scalability as well. The increase in software complexity deteriorates the performance of the vehicle. AVs may perform worse under high penetration of vehicles. Thus, countermeasure the attacks over AVs infrastructure without reducing the performance and complexity is a significant challenge.
l) **Workforce Training:** As the autonomous electric vehicle is a driverless, innovative vehicle with backup support, to give better experiences, the workforce in backend systems is required to have proper training. This training should understand and include the requirement of AVs, ways to train the backup force, define the backup system actors, and list the operational conditions. This way, we can ensure that the operation and maintenance of AVs should be flexible and enhance the performance of vehicles and the overall system.
m) **Cybersecurity and Data Privacy:** In AEVs, communicate between V2Vs, V2I, and V2SD during regular operation. All such types of connectivity require a secure infrastructure and network connectivity. Protecting AVs from hackers is the biggest problem. Hence, there is a need to provide proper protection against data privacy, cyber threats and attacks, and hacking.

2) RESEARCH DIRECTIONS FOR AEVs

The vehicles' challenges are overcome through enhancing the performance. Hence, the following strategies are defined to improve the future development of AVs.

a. Technological developments and innovations in AEVs must involve the technology developers and automakers working on automating vehicles. Similarly, academicians, researchers, and business people need to collaborate so that so many vehicles issues can be solved and solutions can be patentable to enhance the overall performance of vehicles.
b. Sensors can be modified by doing more research and development to detect objects accurately in any weather conditions at the global level and even in bad weather conditions. There is also a need to enhance the accuracy of the detection of objects. As a result, customers can have confidence in their safety throughout the journey. In addition to existing sensors, new inventions and innovations in intelligent sensors are also the latest requirements for interfacing with AI, ML, DL, and ANN. So, these vehicles can operate in any weather conditions without any interruptions.
c. There is a need for prior verification of safety during the operation of AEVs when interfacing with AI, ML, DL, and ANN. A proper safety verification system is required for AI, ML, ANN-based data processors, and decision-making systems so that vehicles can take corrective action.

b) To achieve more consumer acceptance of AEVs, the following factors need to be controlled by taking the proper initiative: socio-economic properties of the vehicle operator, population tally, operation and maintenance of vehicles, completeness of abundance, and vehicle operator enjoyment. Acceptance of vehicles is encouraged by security [187].
c) There is clear-cut technology available in AVs that can easily discriminate the difference between old and new information. As a result, having access to information will simplify the puzzle.
d) The adaption of headlights to all vehicles helps in physically handicaps spot assistance. As a result, AVs can reduce the majority of crashes and also control heavy traffic delays.
e) More accurately, object detection sensors and related innovative technology need to be mature and verify safety and security.
f) Policy, regulations, and legal issues are the main pillars of AVs. For the effective revolution of AEVs, the concerned authorities need to frame proper and legal policies, rules, and regulations.
g) The social acceptability of self-driving electric vehicles can be achieved by employing users who have faith in their safety and security. Thus, user confidence-building programs with live demonstrations are required.
h) Technical knowledge sharing is required with skilled and experienced human resources to rectify technical problems and software errors. The lack of such a skilled workforce is a significant challenge in the autonomous industry. For example, the lack of hands-on training for all backup service providers in blockchain technology is a considerable hurdle to integrate it with AEVs.
i) The price of AEVs is initially high due to a lack of interest in this field's research and development activities. The advancements in sensors, actuators, cameras, wireless technologies, software, hardware, and a large number of recent research and development activities with lump sum manufacturing processes have reduced the cost to a large extent. Further, driverless vehicles also reduce the cost by integrating various optimization algorithms in route identification, performance improvement, fuel efficiency, and many more.
j) The software complexity will be reduced with the integration of intelligent AI, ML, ML, and neural network-based analysis. Further, proper differentiation of each software system and its functionality is required. This clarification can overcome the complexity of software operation in AVs.
k) As technology is very rapidly developing in the field of AVs, according to the needs of technology, the workforce of concern needs to be adequately trained. So, they can enhance and optimize the entire operation of vehicles.
l) The vehicles' protection from hackers is important to adapt to automatic cyber threats and attack information sharing and analysis centers. Vehicle manufacturers must also share hacking, threat incidents, cycle rules, and regulations violations with in-vehicle industries. Specific laws should be enacted to govern data access, sharing, and exchanging between vehicle manufacturers, software suppliers, and owners. As a result, there will be greater security and transparency in the system.
m) Adapting sustainable energy sources for the charging of AEVs will reduce the negative impact on the environment and contribute to the sustainable environment [189].

X. BLOCKCHAIN, GREEN ENERGY SOLUTIONS, AND ELECTRIC VEHICLES

Blockchain will transform the energy sector to build a hierarchy of origin sources. The improved traceability speeds up and automates renewable energy certification. Thus, the important long-term renewable power purchase agreements that need 100% green energy certification. Encouraging large businesses to purchase green energy is critical today. With the blockchain, all parties can verify the results. Smart contracts may also be created using this technology, eliminating intermediaries and simplifying the process. Save money and get privacy.

The massive consumption of fossil fuels in transportation, various industries, and power plants is the cause of pollution in the environment. The existing transportation scenario shows that most traditional IC engines are significant contributors to pollution. Hence, it is necessary to produce clean technology and pollutant-free fuels to enhance the overall performance of vehicles by reducing greenhouse gas emissions. Electrification of the transportation sector is an initiative to reduce pollution, increase energy security by accepting new energy sources, and provide better benefits than traditional transportation systems [190]. Electric vehicles can be classified as BOEV, PIHEV, REEV, BV, ZEVs, HEV, FCEV [189], [191]. Figure 12 shows the configuration of a BOEV. It uses the battery as a source of energy. The battery of the EV is charged through a battery charging unit of the grid system. Electric drives system contains the smart power converter and electric machines. Using an electric drive and differential cum smart transmission gear system, the stored electric energy in the battery is transferred into the wheels of vehicles. A smart power converter is designed for two-way power flows from battery to wheel during regenerative braking. Energy flows from wheel to battery under the braking mode of operation. As per the figure 12 configuration, it has been seen that a clutch is not required in a battery-operated electric vehicle like ordinary gasoline vehicles. Using blockchain-based BOEV is illustrated in figure 12, and the interconnections will continuously monitor the vehicle's activities. Listing these activities, their importance, and their sequence can give quick vehicle malfunction

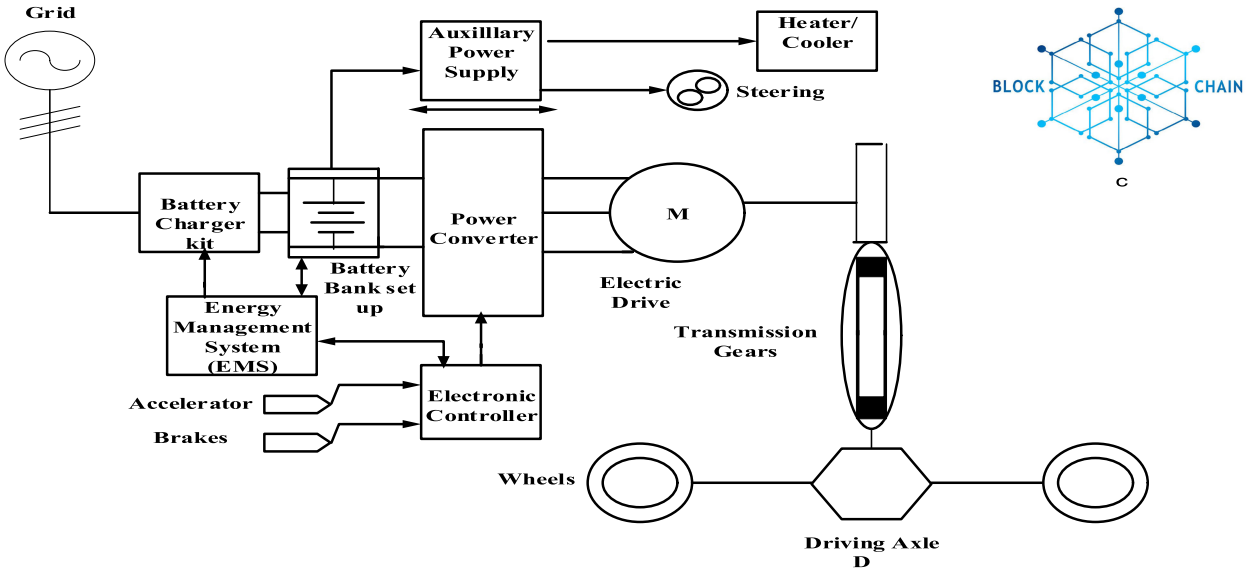


FIGURE 12. BOEV configuration and blockchain.

indications. Further, a pay-asper-usage policy will be easy to implement with this strategy.

FCEV uses both battery and fuel cells as energy sources. The penetration of EVs increases because of variation in voltages, an increase of harmonics, additional overload conditions due to massive charging of EVs, peak load on the distribution network, tripping of protective devices, charging of EVs during peak load is affects the system stability, reduces system reliability and affects power quality. To solve these energy problems distribution system should be adapted [192]. Figure 13 shows the configuration of FCEV. Figure 13 shows that a fuel cell is used as an energy storage device with the help of a hydrogen tank. Step up converter is used to step up the voltage of the fuel cell for charging the battery or storage of electric energy. The configuration of fuel cells such as propulsion systems and drives is similar to BOEV. The energy storage battery unit can provide the sudden and transitory mechanical energy required at the wheel during vehicle operation. The battery unit also helps to optimize the functions of the fuel cell. As fuel cells cannot store the energy during regenerative braking, the battery unit supports energy storage during braking operation. All of these operations and systems (shown in figure 14) are critical to any vehicle. Blockchain can help to monitor and record all of these operations. It would be easy to quickly identify any malfunctioning or change in the vehicle's system operation from its routine using blockchain. The records will be immutable and transparent. Thus, it can help to determine the interruption and its causes at any time.

HEV uses both liquid fuel and battery energy sources, while BOEV uses the battery as a sole energy source. The hybrid (combination of series and parallel) electric vehicle configuration is shown in Figure 14. The main feature of this configuration is a particular gearing smart system, and it is also known as a variable transmission system in continuous operation. This system allows both modes of operation (parallel and series). Like BOEV and FCEV, HEV can also use blockchain technology to interconnect all its systems or sub-systems with immutable and transparent data operations and storage. It helps in continuous monitoring of the vehicle, its activities and helps to avoid any interruption or malfunctioning. Various other important dimensions integrating green energy solutions are:

A. TYPES OF GREEN ENERGY

Due to the enormous penetration in EVs will require additional power generation to fulfill the energy demand by enhancing the other infrastructure of the power sector [193]. Thus, the following strategies are essential to integrating AEVs and Blockchain to solve the energy crisis problems.

a) I am adapting renewable energy sources to power an electric vehicle by improving resource efficiency, lowering emissions, and integrating with the existing electric grid.
b) Involvement of smart grid technology.
c) Involvement of vehicle to grid (V to G) technology and vice versa, i.e. (G to V)
d) involvement of vehicle to home technology and vice versa

Next, factors associated with the integration of green energy sources with AEVs are briefly discussed as follows.

1) INTEGRATION OF RES LIKE WIND ENERGY AND SOLAR ENERGY

Due to the vast potential of renewable energy sources, these sources can be integrated with EVs and grid systems as per the guidelines of the grid codes [194]. Integration of wind energy into EVs and the electric grid is the best initiative for solving the power crisis problems and other technical

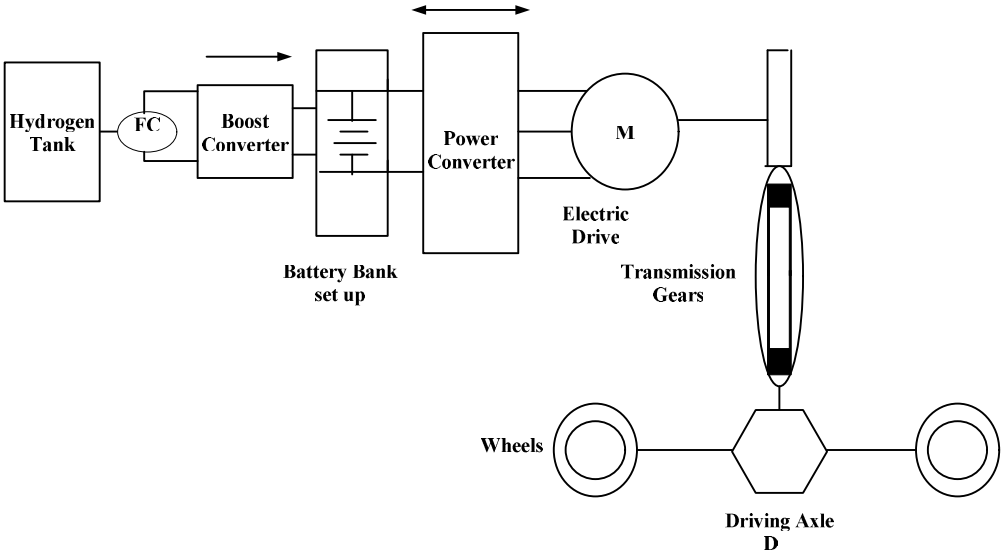


FIGURE 13. FCEV configuration and blockchain.

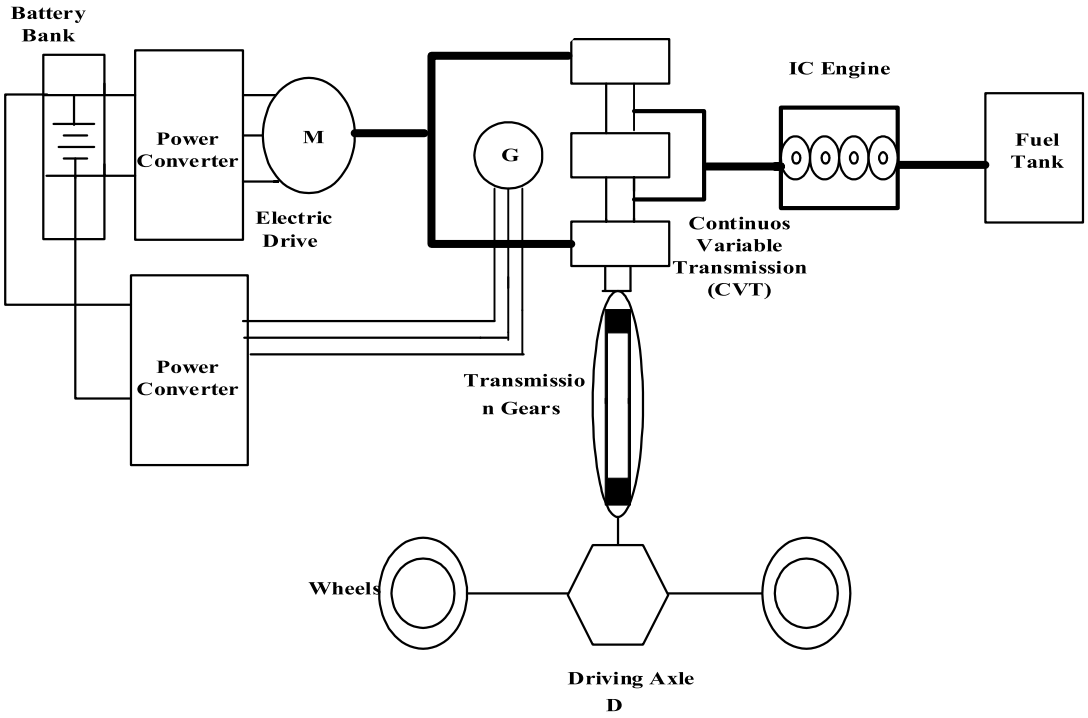


FIGURE 14. Hybrid EV configuration and blockchain.

issues. Wind energy can be used for an offshore and onshore mode of operation for supporting charging stations of EVs, either in an isolated way or in the grid-connected mode of operation [195]. On the shared platform, solar energy is also an excellent option for the integration of EVs. Integrating solar energy, either in an isolated or grid-connected operation, can also be used. Due to grid code constraints, individual solar or wind energy integration into the grid or EVs is the best alternative to combining these two sources. The burden of charging infrastructure and EVs can be decreased with the utilization of RES in EVs. The intermittent nature of RES-generated power can be smoothed out with EV technology.

2) ADAPTION OF SMART GRID TECHNOLOGY

The incorporation of smart grid technologies into EVs, resulting in smart communication mechanisms and intelligent decision-making procedures. With smart grid feasibility integration to EVs, vehicle to grid, grid to the vehicle, vehicle to home, home to vehicle optimization operations can be possible with RES [190].

3) VEHICLE TO GRID TECHNOLOGY (V TO G) AND GRID TO VEHICLE (G TO V)

Extracting optimized energy from RES and accelerate the optimized point into the grid system for EV operation. However, EVs can feed power into the grid, i.e., V to G. In this case, the vehicle acts as an electric load. It draws the power from the grid for the regular operation of EVs, i.e., G to V. During offloading, EVs act as energy storage devices like batteries and supercapacitors and inject the power into the grid called V to G operation of EVs.

4) INVOLVEMENT OF V2HT

In the smart home concept, V2HT is introduced by managing various devices' operations [192]. Whenever there is a long-term power outage or a natural disaster situation in multiple areas, V2HT can be used as an energy source. In the existing power supply network, without significant changes, this technology can be commissioned. It is effortless in construction and easily configurable because it consists of a single EV in-home network [192]. In the present scenario, the major challenge with any type of EV is the power quality issue while integrating it with natural energy sources like wind and solar energy.

B. STORAGE OF GREEN ENERGY

The running time of EVs consumes 70 percent of energy and does not consume energy during the stationary conditions of EVs. Electric vehicles rely mainly on energy storage systems such as batteries, supercapacitors, and fuel cells. In [196], the additional burden on electrical power is highlighted alongside the other power quality issues. Thus, the existing electric grid systems become overloaded with charge and connection to EVs. The RES is used to address this issue, which plays a significant role during peak load demand. The energy storage system drives the electric motor, related axillary apparatus, and other related subsystems of EVs. EVs' driving range and performance are decided by the energy storage system [97], [196], [197]. As a result, the energy storage system is critical in EV operation.

1) ENERGY STORAGE SYSTEMS

The basic requirements of efficient ESS are proper protection, safety, interfacing of power electronics, energy conversion, high discharge time, reliability, and intelligent energy management in distribution systems [196]. Furthermore, different energy sources are used to power EVs based on high energy and high power density criteria. High energy density is used for driving EVs for long-range, and high-power density enhances the acceleration of EVs [189]. ESS is classified as electrical, electrochemical, mechanical, hybrid, and chemical. These systems are briefly explained as follows.

2) CESS

In this case, the storage and release of energy are obtained via the chemical reaction of various chemical compounds in the system. The FC is a chemical storage system that converts chemical fuel energy into electrical energy with a 45 to 80 percent fuel efficiency. FC produces electrical power by using oxidation chemical reactions [190]. FC has various advantages like high-density output, efficient extraction of electrical energy from fuel, no noise, refueling is fast, and emission is more diminutive. The significant challenges with FC include high price, storage difficulty, and voltage drop and loss because of internal resistance [196].

a: EESS

In this case, the electrical energy is directly stored in the form of an electric or magnetic field [196]. The supercapacitor is an example of EESS. A supercapacitor's energy capacity is relatively high (certain kilo farads) compared to an ordinary capacitor. The efficiency of a supercapacitor is 96%, and its specific energy production capacity is 1500-2100 W/Kg. Compared to other ESS, the life of a supercapacitor is long, and it is about 45 years. As a result, the supercapacitor is used in EVs as a vast energy storage capacity source. It has a long operating time and requires less maintenance. Further, it has the characteristics of fast charging and discharging of the supercapacitor. This characteristic makes this source an energy storage mode during electric braking and the power source for feeding the power during a huge acceleration period under hilling in EVs [196].

b: MESS

MESS is generally used for the production of electrical energy. The flywheel serves as an energy storage device and functions as a motor for storage associated with EV systems. During the generator mode, the flywheel's kinetic energy can drive the generator to produce electric energy. It is light in weight, faster in operation, more energy-efficient for extraction of power under regenerative braking, and rapidly injects a large amount of power in a short time under acceleration requirements. Huge charge and discharge cycles of operation can be obtained over a long period in this situation [190], [196].

c: ECESS

Existing conventional rechargeable batteries are coming under this category. In this case, electrical energy into chemical energy is obtained during the charging. Further, chemical energy into electrical energy conversion is obtained during discharging of batteries. It has high efficiency and less emission, maintenance, and physical change. However, the life of a cell gets affected by energy production or storage using chemical reactions [196], [198].

C. TYPES OF BATTERIES

The integration of IoT and Blockchain with batteries to record the status and ensuring payment as per usages. This section discusses the different types of batteries and their feasibility of interconnection with EVs. Details are presented as follows.

1) LEAD ACID BATTERY (Pb ACID)

These batteries are rechargeable and highly matured. The main drawback of this battery is its handling due to the acid substance, high power to weight ratio, and costlier technology. The energy and power density of the Pb acid battery is 36-41Wh/Kg and 245 W/Kg, respectively [190], [199].

2) NICKEL CADMIUM (Ni cd)

The life of the Ni-cd battery is long. It has vast charging and discharging cycles which is about 1550 cycles. The use of this battery is not safe for the environment and human life because of heavy metal/cadmium in its construction. As per ARAI guidelines [190], [199], it is not recommended in EVs.

3) NICKEL METAL HYDRIDE BATTERIES (NiMH)

The energy storage capacity of NiMH is less, and the self-discharge coefficient is high. It has no memory effect. The energy and power density of the NiMH battery is 65-85 W/Kg and 145-205 W/Kg, respectively. The life of NiMH is affected primarily because of long-time storage and its capacity deterioration. This problem can be overcome by mandatory timely charging and discharging the battery before its reuse operation [190], [199].

4) SODIUM/METAL CHLORIDE BATTERIES

It is a ZEBRA battery, i.e., Zero-Emission Battery Research Activities. It has a high-speed energy density. The molten salt electrolyte is used, which is operating at 250-360 degree-Celcius. The main demerits are safety and storage issues during its long period of operation. The energy and power density is 95-125 Wh/Kg and 160 W/Kg, respectively. Unlike other nickel batteries, sodium batteries have enough cycling capabilities and a lesser self-discharge rate [190], [199].

5) LITHIUM-ION (Li-Ion)

Li-Ion battery has huge energy storage capacity, and the ratio of energy density to weight is also better than other batteries. However, it has issues like overheating, high cost, and limited life. This battery is more suitable for EVs because of its lightweight and very high efficiency. The energy and power density is 140-200 Wh/Kg and 510 W/Kg, respectively. Lithium iron phosphate, Li Ni manganese cobalt, Li cobalt, Li manganese batteries are the subtypes of Li-ion battery [190], [199].

6) LITHIUM-ION POLYMER

It has the advantage of a longer life cycle as compared to a Li-ion battery. However, it faces instability during the discharging of the battery below a certain level and an overload condition. Its self-discharge rate is less, specific energy is about 160 Wh/Kg, and specific power is about 320 W/Kg [190], [199].

7) METAL-AIR BATTERIES

Due to the vast energy density of the metal-air battery, it acts as an alternative to the Li-ion battery. It is the best option for energy storage for future EVs and electric grid applications. Energy density is very high in this case, and it is about 3Kw/Kg which is high compared to ordinary batteries [190], [199].

XI. APPLICATION AND USE CASES OF BLOCKCHAIN FOR AGVs

Following the adoption of Blockchain in Bitcoin [200] because of its unique capabilities, several new applications/use cases have been proposed that utilize Blockchain. In this section, three particular examples are highlighted where blockchain technology is helpful in the AGV business. Three uses case are:

Use Case-1: Using blockchain ability to rationalize centralized payment to AGV vendor based on AGV performance in the Global Warehouse Facilities.
Use Case-2: Smart Contract to enable PM's/CM's of AGV.
Use Case-3: Protecting Counterfeit Issues while using Autonomous Mobile Robots

A. INTRODUCTION TO AGV CURRENT LANDSCAPE IN THE SMART FACTORY

Traditionally humans were operating the forklifts for their material management process to support the material flow inside the warehouse and value addition in the assembly area. It has been a time-consuming process, especially when the industry demanded a lean management principle to support accurate and shortest delivery lead time. This need invented AGVs, and since then, we were able to speed up the material flow process and limiting the need for human interactions. In the author's personnel experience (at Intralox and other industries) as a supply chain manager, he has found that AGV with a better transponder that has IoT or sensor-based capabilities. AGVs will be recognized as an efficient tool for warehouse stakeholders. Figure 15 explains how the AGV is aiding the material flow between different areas within a warehouse, from incoming goods to outbound goods. Generally, the suppliers receive the raw materials through the inbounds dock area and are placed in the staging area. Then, the pickers realize the need to put away the stock from the staging area to the appropriate aisle/bin in the storage area based on the raw materials' ABC classification (internal naming-based classification).

After that, the work order gets created for value-added service; the selectors will again transfer the inventory from the storage area based on the picklist generated from the work order. They will be issued to the work cell-1/work cell-2. Post the value-added activity in each work cell, the finished goods are produced and then will again be moved to the packing area to initiate the shipping or outbound process. Once the goods are finished packing and palletized then, the

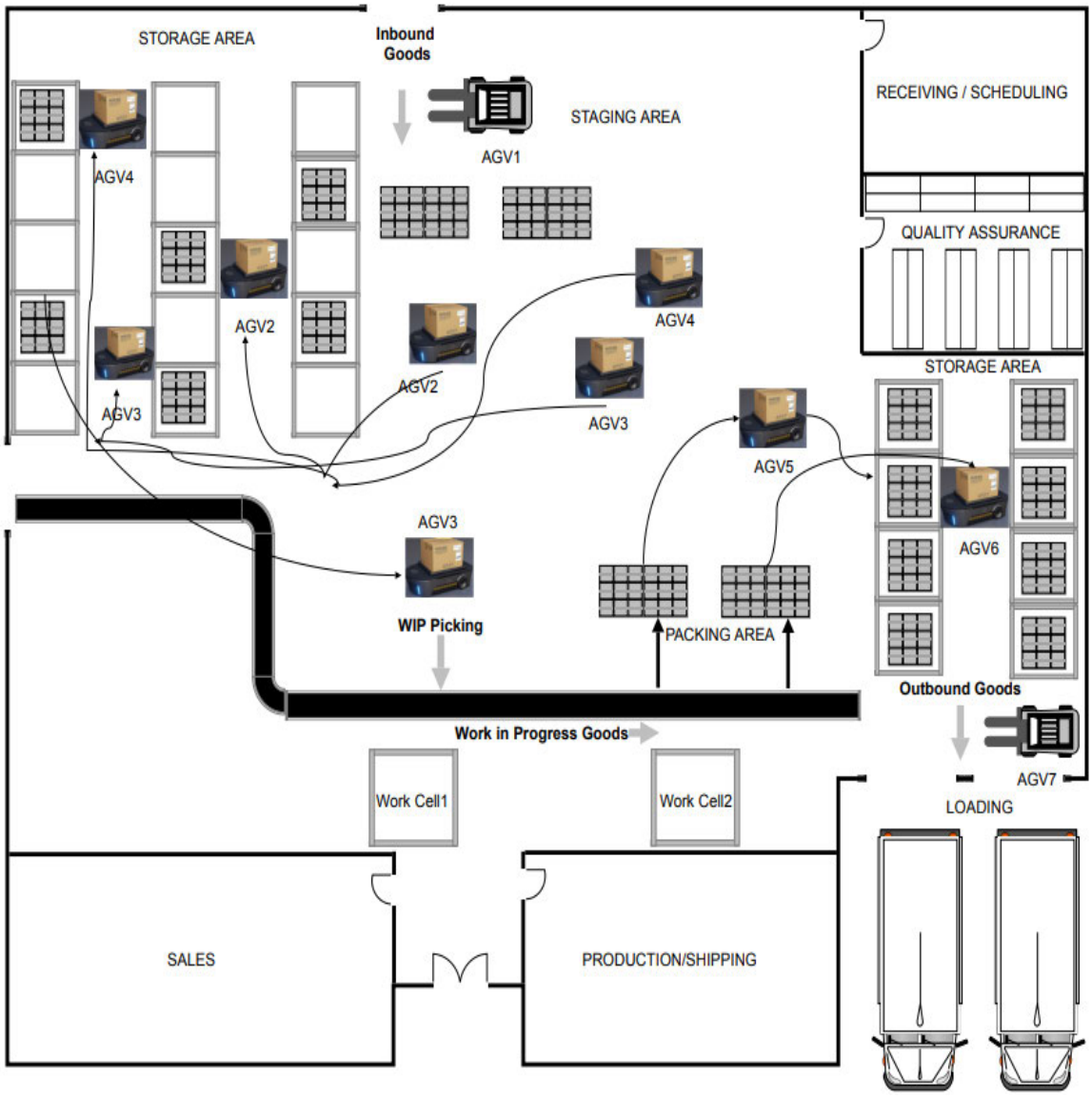


FIGURE 15. AGV aiding the material flow between different areas within a warehouse.

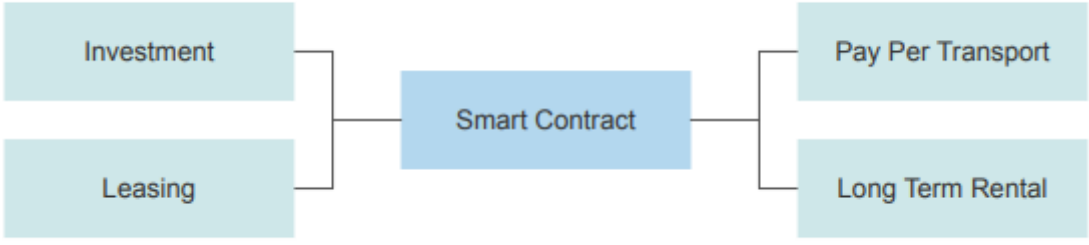


FIGURE 16. Smart contract-based financial options for end-users.

selectors are placed into the storage area. Then, a loaded pick-up is being arranged with the logistic provider. The truck will show up at the outbound dock area at a specific shipment due date to pick up the well-finished pallet. It then is delivered to a particular customer site as per the customer sales order information. Having stated above, the general material flow within four warehouse walls, the conventional way, has generated multiple inefficiency and unproductivity issues due to people/process/technology aspects. Thus, it has further led to few shortcomings in the industry like, (i) unable

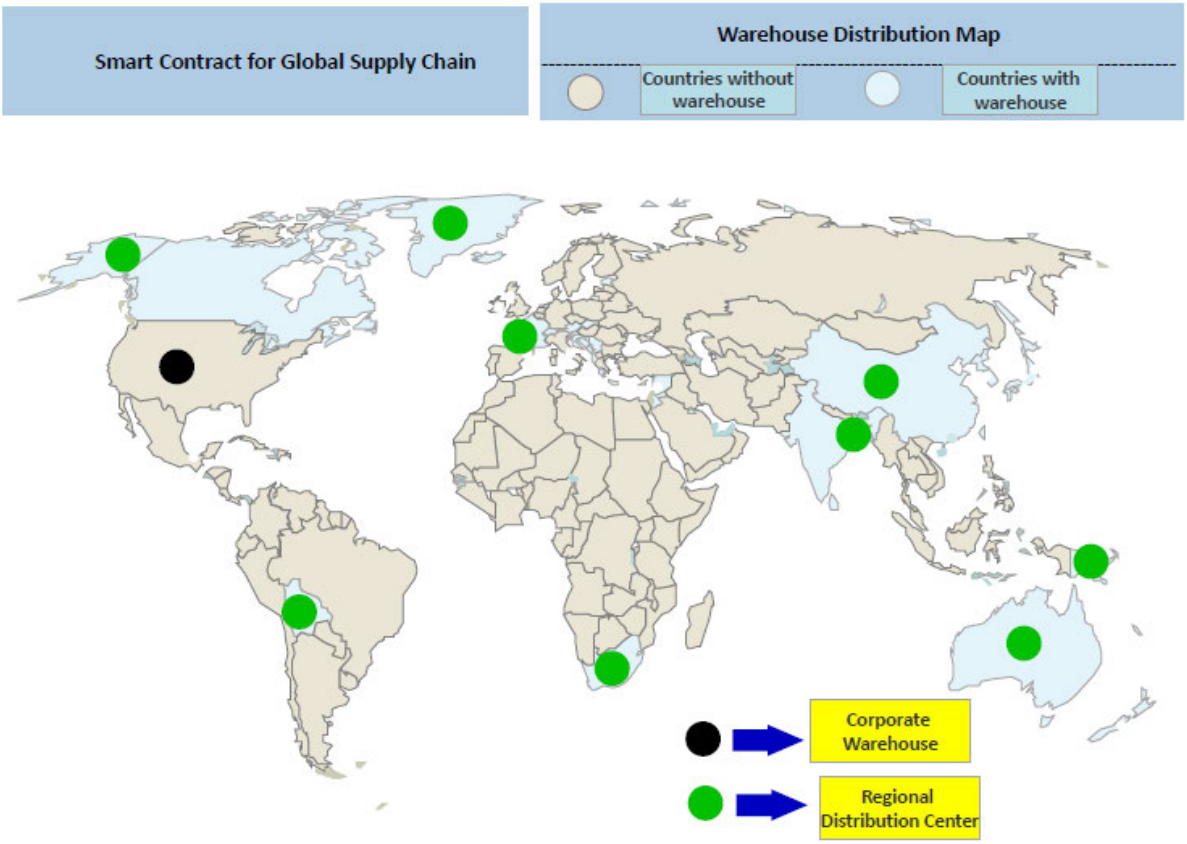


FIGURE 17. Sample global warehouse distribution map.

to keep with the demand between the customer and the order fulfillment process, (ii) modularize the process as the industry continued to build heavy dependency on pickers availability, and (iii) their skill sets along with the inability of the technology to support the velocity of material movement safely and timely. However, AGV's invention has revolutionized the warehouse industry to some level. Therefore, the gaps need to be addressed when it comes to the governance of AGV, interoperability standards between the AGV vendor and the End-user. The counterfeit issues and their impact across the supply chain. In the forthcoming sections of this article, we will see how we can use blockchain technology to meet all or some of these shortcomings in the current industry landscape, as mentioned above.

Table 9 shows the comparative analysis of recent studies on AGVs [201]–[206]. It has been observed in recent studies that there is a lack of proposals in integrating blockchain technology with AGVs. Few discussions over blockchain technology properties are available, which give an introduction to blockchain for AGVs. However, an in-depth analysis is required to take its full advantage. In other observations, AGVs' work is primarily focused on its movements, object detection, path planning, success probabilities, usage in a warehouse, and performance analysis.

B. USE CASE-1: USING BLOCKCHAIN ABILITY TO RATIONALIZE CENTRALIZED PAYMENT TO AGV VENDOR BASED ON AGV PERFORMANCE IN THE GLOBAL WAREHOUSE FACILITIES

Conventionally, when the manufacturers of AGV build their brand AGV's, their design /architecture/manufacturing is always constructed around to suffice the need of the end-users to increase their productivity in material handling and management and improve their manufacturing facility and production flows. In the past, AGV manufacturers always sold their machines to customers at outright rates. Still, as the industry grows and more and more competition drives the market, in the future, end-users will be paying AGV manufacturers based on various financial options. In the author's personnel industry experience, he observed that some AGV vendors are in primitive stage to enable different financial options like a) Pay per Transport b) Long Term Rental c) Investment d) Leasing option, When the AGV automates the transportation of goods from point A to point B, depending on the number of trips in a warehouse shift, the AGV vendor could be paid using the ''Pay Per Transport'' mode, and this is equivalent to RaaS model (Robot-as-a Service). Meanwhile, some end-users were choosing for the ''Long Term Rental'' contract with AGV Vendor to increase payment frequency and minimize repeating admin hassles, where

TABLE 9. Comparative analysis of recent studies over autonomous guided vehicles.

Author	Year	A	B	C	D	E	F	G	H	I	J	K	Major Findings	Major Shortcomings and Challenges
Cupek et al. [201]	2020	✓	×	×	×	×	×	✓	✓	✓	✓	✓	Discussed mainly the applications of AGV and collaboration with other technologies like robotics, artificial intelligence, machine learning, IoT and cloud computing.	This is largely a discussion work rather than making any proposal, simulation or implementation.
Çatal et al. [202]	2020	×	×	✓	×	×	×	×	✓	✓	✓	×	This work has largely focused on the experimentation to learn both the prior and posterior models for AGV to recognize the environment using RGBD camera.	This work has largely focused over anomaly detection in Bayesian surprise-based implementation. Work can be extended to integrated advanced technologies (like blockchain)
Ana et al. [203]	2020	×	×	×	✓	×	×	✓	✓	×	×	×	This work is focused over wireless control of autonomous vehicles. Here, reinforcement learning is integrated to find the optimal speed and achieve the mission path in shortest time duration.	This work is helpful in identifying the performance parameters and their evaluations for remote control of AGV but it does not say anything related to blockchain or security.
Sánchez-Sotano et al. [204]	2020`	✓	×	×	×	✓	✓	×	✓	✓	✓	✓	This is a survey work that discusses the use of important technologies associated with shipbuilding Sector. Here, both AGV and blockchain discussion are done briefly.	This work is more of a theoretical discussion and related developments. No discussions over how to implement the advanced technologies is performed.
Wang et al. [206]	2020	×	×	✓	✓	×	×	✓	✓	✓	×	×	This work has implemented a clutter-resistant SLAM algorithm for AGVs. The performance of AGVs is tested in real environment.	This work has also not discussed the importance of blockchain technology. Here, main focus is over the operation of AGVs rather than elaborating the security-related issues.
Stillig and Parspour [205]	2021	✓	×	×	×	×	×	✓	✓	✓	×	×	This work discusses the application and usage-based analysis of AGVs. A mathematical discussion is compared with manual processed to discuss the advantages.	This is a short analysis to understand the importance of autonomous system especially for car interior parts production. A detail implementation, or solution-based approach is required to address the recent challenges.

A: short survey, B: Long and in-depth survey, C: Implementation-based study, D: Simulation-based study, E: Blockchain proposal discussions, F: Smart contract, G: Power-issues, H: Infrastructure Requirements, I: Supply Chain Management, J: IoT, K: Cloud/Edge/Fog computing.

the payment is based on monthly rental with the commitment/contract being created for at least a year or two between the two parties (AGV Vendor and AGV End User). There is also a ''Leasing'' option; as part of the lease fee, the vendor could also cover the preventive and corrective maintenance for AGV during the lease period. Still, some liabilities will be applied to end-users if the AGV system is wrongly used or some system damages occurred during its operation within the warehouse. The last option is the little choice among the AGV end-users. It puts them in the traditional CapEx approach to operate their relationship with any system or technology vendor where they invest in this technology. Thus, ownership now lies just with AGV end-users to buy all the system components and tangible assets. Due to multiple factors involved with each financial option and within each option, since it is entirely manual, there are many opportunities to have scope creep and shortcomings when tracking the performance-based pay for the AGV vendor. Here, a blockchain-based smart contract can be established between AGV vendors and AGV end-user, as shown in Figure 16.

Further, it comes to end-user who has global supply chain operations, as shown in Figure 17. The contracts must be established for local warehouse facilities in each country, which are bound by the local legacy factors. Blockchain technology could play a vital role in establishing the smart contract by the centralized executive team sitting in the corporate headquarters (e.g., US). As shown in figure 17, globally, warehouse facilities are present in many countries like the USA, Alaska, Brazil, Argentina, UK, Germany, India, South Africa, China, Australia. Each warehouse facility has different requirements, sizes, layouts with other local regulation laws, needs for maintaining multiple vendors for each warehouse's AGV, and difficulty in the ongoing operations of AGV. All of these add more technical and admin debt to the corporate. Using the blockchain distributed ledger technology for the payment gateway concerning the smart contract

will bring more traceability and process efficiency across the supply chain for the global supply chain entity.

A sample warehouse facility (as shown in figure 15) is considered for scenario analysis to explain the AGV-related parameters and justify the performance of AGV. In the scenario, the considered parameters are associated with the performance of the AGV, how it is benchmarked with current manual operating cost, and how all cost and performance-related calculations could be embedded into a Smart Contract for a blockchain-enabled payment gateway. Following are the parameter considerations to calculate the cost of operating the AGV in each warehouse.

- ***AGV Electric Consumption per year***: This depends on the type of battery being used in AGV. The electricity usage for charging the AGV battery per year as a single AGV could use many batteries in a year.
- ***Rate of Electricity per unit***: This is measured as the electricity cost per kilowatt-hour (kWh) where the direct cost of the AGV investment decision. This rate could vary depending on the industrial schemes in each country or their geographic location for each warehouse.
- ***The number of shifts in the warehouse***: is computed as the total number of transitions of material management operations in the warehouse. Some warehouse could run their material management operations twice or thrice. Thus, this factor is also an important factor to determine the usages of AGV and its impact on the entire order fulfillment operation.
- ***Charger Efficiency***: This is an indirect factor that affects the performance of the AGV in the long run as it could positively or negatively impact the total operating cost when it comes to battery life and its replacement costs.
- ***Number of Operators per shift***: This is measured as the number of warehouse pickers per shift. It could be vary depending on the warehouse size and the volume of order fulfillment required in each warehouse.

In addition to the above parameters, few factors need to be in-built in the Smart contract depending on the picking and the Packing process [207]. These parameters are briefly explained as follows.

- ***Setup Time to Start and Complete a batch (generally measured in Seconds):*** This is calculated as the time required to set up AGV to arrange for transportation to pick or drop off a load within the warehouse.
- ***Total Time To Pick and Order line from a location (generally measured in Seconds)***: This is calculated as the actual transportation time required to move the box or pallet from the Staging area to the Storage area or from the Storage area to the Work-in-progress area.
- ***Average Number of Distinct Items in a Single-Item Order Batch***: This is measured as the average number of items transported. It could vary depending upon whether the picking is batch picking or cluster picking.

Based on Table 10 sample data, the importance of AGVis was analyzed and compared to the manual process. Equations (i) and (ii) are proposed for measuring the performance and cost. Details are discussed as follows.

$$\begin{aligned}&\text{AGV Cost Computation}\\&= \text{AGV Electric Consumption per year}\\&\quad * \text{Rate of Electricity per unit}\\&\quad * \text{Number of shifts in the warehouse}\\&\quad * \text{Charger Efficiency} * \text{Number of AGV's installed.} \qquad \text{(i)}\end{aligned}$$

$$\begin{aligned}&\text{Current Manual Operating cost}\\&= \text{Operators Renumeration} * \text{Number of Operators per shift}\\&\quad * \text{Number of shifts in the warehouse.} \qquad \text{(ii)}\end{aligned}$$

The comparative analysis of two factors shown in equations (i) and (ii) evident that the cost of AGV (54,000$) is less compared to manual (900,000$) for a year, and the performance of AGV is much better than operating in a manual world. The above calculation can be embedded with other parameters in Etherum supported Smart Contract, deployed in the blockchain network. AGV makers, AGV end-users, and power utilities can all use the newly built smart contract. Using these calculations, they will manage the terms and conditions for each financial option that AGV end users have selected to run their warehouse operations. Hence, increase efficiency and productivity. Finally, it can be used as a payment gateway for AGV vendors to pay based on AGV performance when operating in the global warehouse supply chain model.

C. USE CASE-2: SMART CONTRACT TO ENABLE PM/CM OF AGV

In reality, after the AGV has been sold in multiple units to a global supply chain warehouse, the data structures for the assets might be complicated. Thus, it is difficult to track a smart contract between AGV manufacturers and end-users. Thus, there is a need to establish a maintenance contract (for both PM and CM) to ensure that the spare parts replenishments happen based on the smart contract supply chain. Further, a smart contract can provide the yearly maintenance payments though the hyperledger is contingent upon the asset's health.

AGV remote assistance can solve two problems (spare part supply chain management and payment gateways) using blockchain technologies. Today, the ability for remote service is minimal, or in other words, it is entirely manual. Further, it is the AGV vendor who decides when to visit the installed sites. Usually, it is periodical to perform both corrective and preventive maintenances regularly. In the present scenario, the IoT and sensor-based technologies are installed on top of AGV to improve the current situation. However, there are still some shortcomings in performance improvement, cost, and remote assistance. The IoT-based sensor could help monitor the performance and the usage of operational parameters (of AGV) remotely. Still, it cannot trigger the spare parts needs if any parts need to be replaced as preventive maintenance. Also, the payment is very contingent on the success criteria

TABLE 10. Parameters to calculate and compare the performance of AGV with the manually run warehouse [158].

Parameter	Description	Value
AGV Electric Consumption per year	Electricity Consumption for charging the AGV battery per year	500 kWh
Rate of Electricity per unit	Electricity cost per kilowatt-hour(kWh)	13 cents
Number of shifts in the warehouse	Total number shifts of material management operations in the warehouse	3 Shifts
Charger Efficiency	AGV Charger Efficiency	90%
Number of AGV's installed	Total number of AGV's installed in the warehouse	3
Number of Operators per shift	Number of pickers per shift	5
Operators Renumeration	Renumeration paid to operator per month	60,000 USD

defined in a contract between the AGV vendor and AGV end users. Presently, it is a manual process. Hence to overcome these shortcomings, the below could be explored in the AGV industry with blockchain technology.

a) Spare parts supply chain using smart contracts.
b) Hyperledger for payment gateway.

The smart contract for PM depends on the critical parts mentioned in table 11 [208], [209]. Table 11 provides the sample list of essential elements, their manufacturers, and prices used in the AGV. These parts can be covered in the AGV maintenance contract established between the AGV vendor and AGV end-user. In [208], this information is used for estimating the cost of a maintenance contract. Depending on the spare parts needs and based on the price of each spare part, automatic payment via the blockchain payment gateway will be enabled to improve the efficiency of AGV's preventive and corrective maintenance process.

D. USE CASE-3: PROTECTING COUNTERFEIT ISSUES WHILE USING AUTONOMOUS MOBILE ROBOTS

There is a growing research trend in AMR, especially at pilot-to-industrial scale for packaging and delivery in the food industry's supply chain leading to smart packaging and smart last-mile delivery to the customer. Figure 18 shows a similar example of pilot-to-industry scale usage. In the packaging system, a small wire is embedded in the package label. This wire is nothing but a transmission system for RFID tags, and this will act as proof of delivery for the seller [173], [174], [209]. An RFID reader or application can read this tag to authenticate the product that has been received by the customer and subsequently make the digital payment using the cryptocurrency. In RFID reader and tag-based systems, lightweight cryptography primitives and protocols are used to ensure security. The lightweight authentication protocols create a new authentication key which is automatically updated in rewritable tags. The lightweight authentication protocol helps the reader or application to understand the new key. This key can be stored on a Hyperledger-based blockchain for the public to purchase and use the product. In a blockchain network, smart contracts are also executed. It helps the parties. For example, a smart contract can automate end-users to purchase the product after verifying its date, time, location, and historical production and transportation. An end-user will get more product information like the picture of a product, packaging quality, and historical scans of the product during its supply chain process. These mechanisms ensure the safety, quality, transparency, trust, and originality of the product. Blockchain keeps a record of every activity that happens in its network. Thus, storing the authentication key in the blockchain network ensures that every action associated with it will be recorded. Using this feature, AMR can assure customers that the product they purchase is authentic and authenticates from its historical information, from production and packaging to its sale. This procedure ensures guard against counterfeiting, corruption, or having any other counterfeit issues such as if the products have been appropriately handled or not across the spectrum of supply chain depicted in figure 18.

XII. BLOCKCHAIN FOR UAeV

UAeV is an aircraft that does not have a human pilot. UAeVs, sometimes called "drones," can be completely or partially autonomous but are usually operated remotely by humans. An UAeV is a vehicle that propels itself independently, remotely, or both. It is equipped with sensors, target agents, offensive munitions, and electronic transmitters to intercept or destroy hostile objectives. Because they are not restricted by the life-assistance equipment or design-security constraints that manned aircraft face, UAeVs can be highly efficient, providing significantly greater scope and endurance than similar manned systems [19], [210], [211]. UAeV application fields have grown with their popularity, and in many circumstances, a cluster of UAeVs can fulfill the functions of a specific application. Only a few examples include disaster relief, monitoring, network relaying, and the discovery of energy-efficient equipment [212]. While UAeV coordination is important for many applications, most current schemes lack a global information-sharing platform for UAeV network members, relying on local communication between neighboring UAeVs [213]. Therefore, blockchain technology can help, enabling a new line of research into unmanned aerial vehicle networks by emphasizing a global communication channel. Each UAeV must transmit accurate real-time data on its location, flight path, and any planned changes to

TABLE 11. Sample price list for the AGV maintenance provided by the AGV Supplier [158].

Search Code	AGV Supplier Part Number	Description	Original Equipment Manufacturer (OEM)	OEM Part no.	Price (USD/Each)
1	AGV-Engine	AGV Engine	AGV Mfr1	ENGINE-X123	650
2	AGV-RFID	RFID Reader	SIEMENS	XX321	1200
3	AGV-Pin	Pin Hook	AGV Mfr2	W-09546	1300
4	AGV-Wheel	Traction Wheel	Best Wheels	B95678	1800
5	AGV-Filter	AGV Oil Filter	Filters Inc	54389076	120

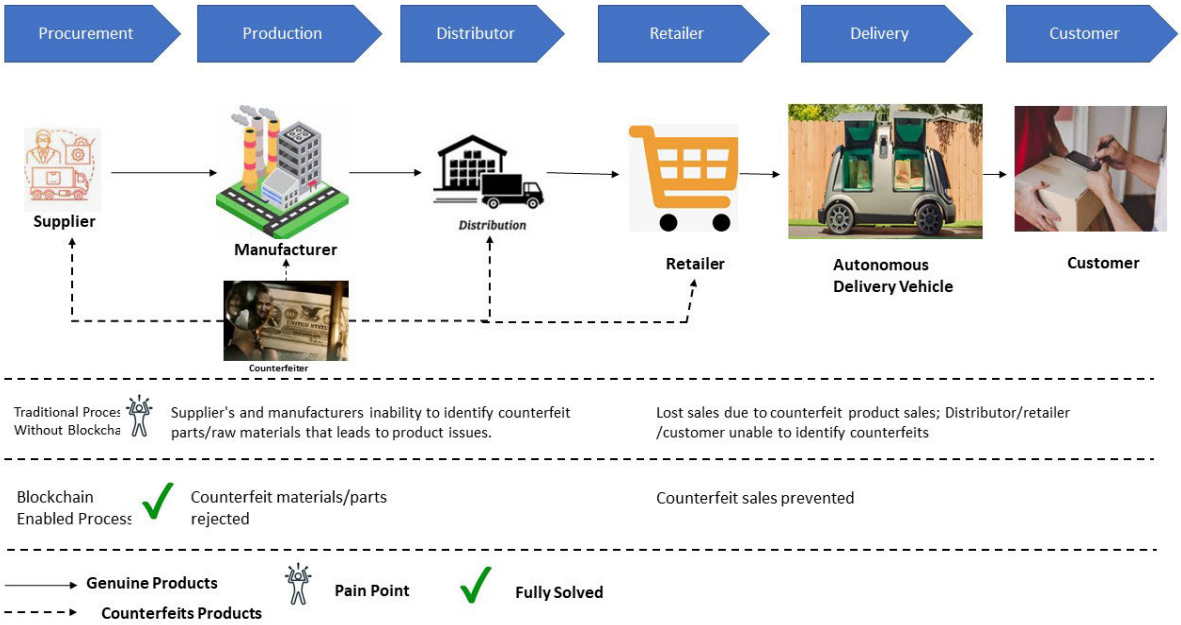


FIGURE 18. Autonomous mobile robots in pilot-to-industrial scale usages.

congested airspace. Previously, drone operators were held responsible for this, but blockchain offers an alternative solution. By assigning a unique ID to each uncrewed aircraft, the blockchain can keep a "real-time record" of its position and speed, as well as its operator and maintenance history. Blockchain enables smart contracts and ensures high supply chain trust, transparency, efficiency, and security. The participants in the contract shall negotiate according to the rules established in the smart contract. When the predetermined rules are met, the agreement automatically enters into force. These smart contracts contribute to the verification process, facilitation process, and enforcement of transaction engagement. Thus it allows for decentralized automation.

UAeVs conducting inventory management functions can rapidly transfer data to blockchain-connected cyber-physical systems. Every block on the blockchain will comprise information about inventory supplies scanned by the UAeV and additional timestamps, making the process of storing and tracking things easier. UAeVs can be designed to charge and check at predefined periods, automating the storage and verification [214]. Smart contracts can be used to automate specific transactions and operations, such as ordering new supplies when a product's stock falls below a certain threshold. Smart contracts are executed without the need for human involvement when specific predefined criteria are met [215]. Smart contracts enabled by blockchain technology help automate compliance with unmanned aircraft regulations. This gadget can reduce human error by preventing planes from flying higher than 400 feet or requiring planes to remain within a predetermined radius of an airport. Blockchain can be used to track drone maintenance and defects. When a flaw is detected, a smart contract will need to be signed using a technician's private key before it can continue flying. In the event of an incident, blockchain enables more comprehensive audit ability across the system. Changing flight records is more difficult on a decentralized blockchain, and multiple blockchain nodes provide data redundancy. Blockchain ledgers can restrict private or consortium blockchains' access to proprietary data such as flight plans and operator details. Blockchain technology creates a permanent and accessible

record, and it has the potential to reduce the number of paperwork required in aviation today significantly [216].

According to the FAA, in 2019, approximately 412,000 commercial drones were registered in the United States [217]. The combination of Drones with blockchain technology can change the way we live. The use of blockchain has the potential to improve the usability of UAeV-based applications dramatically. As stated by UNICEF, about 73,000 people were killed in the October 2005 earthquake in Pakistan. Government, military, and civil aviation officials reacted swiftly, but their efforts were supported by cutting-edge aerial networks operated by drones, which allowed more advanced rescue assignments in remote villages [218]. Governments worldwide can use blockchain to track the identities of UAeVs traveling across their borders. The next generation of UAeVs must be designed to operate in an environment full of obstacles and the threat of cyber-physical attacks. UAeVs are classified according to their functionalities and features. The functionalities vary according to the intended applications, including aerial mapping, surveillance, agriculture, scientific research, and photography [219]. The UAeVs are classified by their capabilities, flight endurance, and size [220]. Primarily the UAeVs are multirotor, fixed-wing, single rotor helicopter, and fixed-wing hybrid VTOL. These UAeVs are briefly explained as follows.

- ***Multirotor UAeVs*** are used for video surveillance and photography. It is easy to manufacture and cost-intensive. However, Multi-Rotor UAeVs suffer from limited flying time, speed and endurance. Further, it spends most of its energy to stabilize the air.
- ***Fixed Wing UAeVs*** never use the energy to fight with the gravity of the air, and the operators are required special training. However, Fixed Wing UAeVs need the runway or parachute to land on the ground safely. Further, it is costly.
- ***Single Rotor Helicopter*** design structure very much similar to the helicopter, and the operators required special training. However, single rotor machines have higher complexity and cost. Further, the UAeVs handle carefully; otherwise, it involves in the accident.
- ***Hybrid VTOL*** is a term that refers to the combination of fixed-wing and rotorcraft. This model is critical for both manual gliding and automation. The aerial vehicle is thrown into the air from the ground leveraging a vertical lift. In autopilot, gyros and accelerometers are employs to stabilize the vehicle in the air [221].

Further, the UAeV's can be classified based on various characteristics such as weights, maximum altitude, wing loading, endurance, and range [222]. Apart from these classifications, military-oriented UAeVs have different types of UAeVs based on their military mission capabilities. According to Watts *et al.* [220], the UAeVs are MAV, NAV, VTOL, HALE, LASE, and LALE. Gupta *et al.* [223] classify the UAeVs based on the Altitude, endurance, and range such as MAV, NAV, MUAV, MALE, HALE, and TUAV. Cavoukian [224] classify UAeVs into MAV, TUAV, and strategic UAeVs. The TUAV are further classified according to their range, including short, medium, close, MALE, and long-range endurance. Zakora and Molodchick [225] classified the UAeVs according to their range and weight, including MAV with a short-range, Lightweight UAVs with a small range, Lightweight UAeVs with a Medium range, Average UAeVs, Heavy medium-range UAeVs, Heavy UAeVs with an extensive range, and unmanned combat aircraft. Therefore Table 12 depicts the classification of UAeVs according to their range and weight. Thus, the importance of blockchain classification is discussed.

With advancements in electronic devices such as batteries, microprocessors, sensors, and navigation systems, optimizing the cost and weight is possible. Thus, a variety of UAeVs is employed for civilian and military perseverance. The UAeVs are classified based on performance metrics like production costs, engine types, endurance, weight, wingspan, speed, wing loading, range, and maximum altitude. The UAeVs are classified as Landing, Helicopter, Hybrid models, Heli-wing, and Unconventional types. These UAeVs are briefly explained as follows.

- ***Based on Landing***, the UAeVs are further classified according to their landing style into HTOL and VTOL. The HTOL is leveraged to balance the mass, maintain stability in the air, and control. The propulsion model in HTOL is designed at the rear of the fuselage through the tailplane forward, tail plane-aft, tailless, and tail-aft on blooms [226]. Therefore, the landing and take-off are performed horizontally. In VTOL, the propulsion system is located in front of the fuselage. Thus, landing and take-off are performed vertically, and VTOL provides more efficiency than HTOL [219], [227].
- **Hybrid models** combine the HTOL and VTOL capabilities using tilt-wing, tilt-rotor, tilt-body and deduced fan. The rotors are oriented vertically; in cruise flight, they are oriented 90° tilted. The engine wings are either fixed or tilted in a tilt-wing configuration. The wing can rotate from 0 to 90° to adjust the engine orientation from horizontal to vertical [228]. Tilt-body aircraft are different from fixed and rotary wings. The wings have complete freedom to rotate from the left or right to the body's center [229]. The deduced fan consists of two contra-rotating elements that optimize the body rotation [227].
- ***Helicopter*** design structures are employed by hovering flight with VTOL UAV. The helicopter UAVs are classified as single rotors, coaxial rotors, tandem rotors, and quadrotors [230]. Single rotor helicopter UAV is the most common type, which uses the tail rotor to counteract the engine tilt momentum. A tandem rotor, alternatively referred to as a dual rotor, is composed of two rotors placed at the front and rear of the flight. The rear rotor is put in a higher position than the front to avoid collision between the blades. Coaxial rotors

TABLE 12. Blockchain and UAeVs classification according to weight and flying range.

S.No.	UAeV	UAeV Class	Weight range	Flying Range	Blockchain Usages and UAeVs Classification
1	NAV	Fixed Wing, Multi Rotor	<=200g	5km	Blockchain technology can be used with UAeV classifications in following ways: • UAeV's features (weight, class, flying range) based identification, tracking and monitoring can be performed using IoT network and data can be securely stored in distributed ledger createdusing blockchain. • Individual blockchain (e.g. private or consortium) can be created for each UAeV device to track its performance and can be priced based on its utility and performance. • Automatic execution of functionalities and transactions in UAeVs can be performed using smart contracts. • UAeVs integrated with multiple applications (e.g. supply chains, aerial monitoring, tracking) can help in faster data collection and sharing with blockchain networks. • UAeVs with lightweight cryptography primitives and protocols can help to securely collect the required data and exchange with authenticated users. • Pay-as-per-service model can be applied effectively. For example, UAeVs deployed for some mission can be charges for successful completion of their jobs. • UAeVs can be used as router or repeater in intranet or internet. This feature extended thepossibility to create network in remote areas as well.
2	MAV	Fixed Wing, Multi Rotor	200g-2kg	25km	
3	MUAV	Fixed Wing, Multi Rotor	2kg-20kg	40km	
4	Lightweight UAV	Fixed Wing, Multi Rotor	20kg-50kg	70km	
5	Small UAV	Fixed Wing	20kg-150kg	150km	
6	TUAV	Fixed Wing	150kg-600kg	150km	
7	MALE	Fixed Wing	600kg-1000kg	200km	
8	HALE	Fixed Wing	600kg-1000kg	250km	
9	Heavy UAV	Fixed Wing	200kg-2000kg	1000km	

employ two rotors placed one upon the other on the same axis, and rotation is in a different direction. The quadrotor has four rotors mounted at the tandem wings.

- ***Heli-wing*** is another type of UAV that leverages the rotating wing as a blade. This type of UAV flies vertically with a fixed-wing.
- ***Unconventional type*** UAVs are bio-inspired flying robots designed and fabricated with the inspiration of birds and insects. Thus, these birds or insects are controlled through electric chips. The bio-drones are classified as taxidermy, live and hybrid drones. Taxidermy is the practice of using the birds as flying models or dead animals [231]. The live bio drones are being developed to optimize the electric circuits in conjunction with neurophysiology research and control birds and insect flights [232]. The Hybrid drones are designed and manufactured in various environments and can walk and move on land, water, swimming, and diving underwater [233].

A. BLOCKCHAIN AND UAeVs

Recent times have witnessed several advances in UAeV, physical design, and networking technology, paving the way to their wide application in various industrial, commercial and civil arenas. UAeV technology has demonstrated tremendous potential to revolutionize warfare and enabled applications in surveying and mapping, agriculture, asset inspection, video surveillance, and aerial photography. UAeVs have been widely deployed in smart city scenarios as well. In critical strategies, particularly in hostile areas and in hazardous environments, they are widely used. As per a projection, the number of devices connected to the internet will rise by 30.9 billion by 2025. Prediction is that a large percentage of these devices will be vehicles [234]. The connection and cooperation of smart vehicles and devices in a network delivers several successful use cases and industry 4.0 applications in agriculture, health emergency services, traffic monitoring, and infrastructure inspection. UAeVs are smart, flying objects with sensors and software systems designed to accomplish a complex mission. Wide variation in size, complexity, functionality, precision, communication capability, and sensing ability is noted, as per the domain of deployment and operation. Multi and Cooperative UAeVs are other emerging areas. Usually deployed in open environments or diverse smart city setups, UAeVs tend to become vulnerable to being lost, damaged, destroyed, or hijacked [19].

As applications of UAeVs increase by multiples recently, some of the issues around data security need addressing. UAeVs operate in distributed and untrustful environments. They are vulnerable to various attacks as they have numerous onboard sensors that gather data. An attacker can gain access to sensitive sensory data and use it for fraudulent tasks. On reprogramming, it can be turned into a vector to plan undesirable activities and cause irreversible damage to society [235]. Blockchain as an emerging technology has been offering solutions to security concerns of the internet of vehicles. It guarantees trust between UAeVs and their relevant base stations, provides decentralized data, accessibility, immutability. The distributed ledger blockchain protects shared data using cryptographic techniques, public-key encryption, and consensus protocols, ensuring the truthfulness of stored data and allowing transparent and secure access [19]. Integration of blockchain in UAeV builds the foundation for several new applications, providing the desired level of security and privacy. It is a strongly evolving area of research, revealing insights, underscoring challenges, and opening up opportunities to future research. Alladi *et al.* [19] presented a review of various applications of blockchain in UAeV networks. They discussed challenges and suggested future directions. Alvares *et al.* [236] submitted a detailed study on blockchain-based solutions for UAeV assisted connected vehicle networks in smart cities. They focused on the challenge of resource constraint in connected IoVs, as blockchain implementations' energy and computational needs are hard to suffice. The work outlined open challenges and future perspectives. [236]. Complex autonomous setups

such as AUVs require high data rates for successful deployment and acceptable quality of service feedback from the end-users. 5G wireless networks provide high data rates and low latencies. 5G coupled with fog, edge, and particularly mobile edge computing (MEC), can provide support for increasing the number of connected devices, irregular data, and service requests, both in low and densely occupied locations. Moayad Aloqaily and co-authors discussed 5G environment for UAeVs integrated with blockchain, proposed their solution with blockchain deployed within UAeV and supported by fog and edge computing, and evaluated their solution against traditional integration UAeV with cellular networks in terms of successful data and message delivery rates. They presented challenges, future research and discussed developments around federated learning [237]. AUeVs/Drones, during the outbreak of a pandemic, Covid-19, have been used in emergency health care, for distributing medicines, necessary good supplies, and food to the quarantined population, supervising social distancing measures, etc. Smooth handling of these tasks depends on collaboration and effective communication between multiple cooperating AUVs. Blockchain integration provides decentralized data access and operation in a controlled environment. Alsamhi [238] discussed the integration of blockchain in multi-drone to successfully combat Covid-19. They presented suggestive frameworks and interventions in blockchain as a solution to the current pandemic and future pandemics. Mário Gabriel Santos De Campos presented a framework for blockchain-integrated multi-UAV for surveillance activities to support coordination between UAeVs and enable safe and secure financial transactions. They proposed IOTA blockchain integrated systems as effective for cooperative mission tasks, being computationally light at the same time [239].

B. CHALLENGES IN UAeVs AND ASSOCIATED NETWORKS

This section discusses various challenges of UAeV. Details of these challenges are presented as follows [1], [2]:

- **Cyber threats and attacks**: According to [1], various cyber threats and attacks occur in UAeV cyberspace, including attacks like hijacking in which an unauthenticated party tries to control UAeVs. In this attempt, vulnerabilities in cyberspace are identified, especially those vulnerable points where it is easy to establish an insecure communication link that causes serious flaws in UAeVs flying. Another vulnerable point in UAeV-based cyberspace is the GP spoofing attacks. In these attacks, the attacker observes signals that either use no encryption mechanism or weak encryption. Additionally, misleading the information to the UAeV system is another important consequence of a GPS-based attack. A GPS-based attack can lead to loss of positional information, which may threaten UAeV devices or the lives of people near UAeV's flying zone. Another severe possibility of a GPS-based attack is jamming the GPS signal. In a jamming-based attack, UAeV is not able to operate or take any kind of support. Thus, this is more dangerous than other cyber attacks.
- **Physical Attacks**: This is another major attack on the UAeV system. There are many reasons for this attack includes a strong wind, extreme temperature variations, highly complex flying zone, and unpredictable flying objects (birds, other drones). All of these lead to physical damage to drone devices. Although various sensors (LiDAR or RADAR) are used for obstacle identification, there are always possible errors in the present scenario. As it is difficult to handle, this attack lies in the significant attack category.
- **Communication link-based attacks**: In the UAeV network, communication links are established between two UAeVs, UAeV and ground control station, and two ground control stations. These communication links are prone to denial of service, traffic overloading, signal spoofing, eavesdropping, identification, and privacy mislead, ad false position-based attacks. In all of these scenarios, an attacker tries to disturb, break or take control of communication links.
- **System-based attacks**: In UAeV or associated networks, there are many systems. For example, Cyber-system to access and coordinate with UAeV devices remotely, cloud computing system for internet resource service management for establishing communication links, database system to fetch, store and retrieve appropriate data, traffic management system, information security system and surveillance and monitoring system. Thus, various sorts of assaults are feasible, including SQL and NoSQL-based injection attacks in database systems, unprotected or insecure application programming interfaces in cloud or communication networks, malware in any system, and brute-force attacks in data hijacking over weak communication lines.
- **Vehicle Privacy and Anonymity**: In coordinated AVs networks, messages sent from one vehicle to any remote vehicle do not ensure to reach in time because of the ad-hoc vehicular network constituted by AVs. Additionally, the vehicle's identity is required to be hidden to avoid identity-based attacks. Traditional security mechanisms cannot ensure this property because of a lack of security properties like immutability, transparency, robust consensus approach, distance bounding, and distributed data storage features. All of these properties can be ensured using blockchain technology.

Additionally, there are many other challenges in blockchain-integrated UAeVs. For example, Wiggers [1] discussed adversaries targeting hardware, software, or communication systems associated with UAeVs. In UAeVs, the software component controls the hardware and apps. After jailbreaking, the mobile operating system, ground control station, or other smart devices are vulnerable to buffer overflow or code injection vulnerabilities. An attacker may use these flaws to get access to services or even control the UAeV.

A hostile actor may direct a UAeV's weapon towards specific targets, alter data, or insert false information. Security measures must prevent unauthorized access and malicious code execution during startup and operation. Attackers target UAeV payloads like cameras and global positioning systems. By faking positions, an opponent may change the mission path or capture the UAeV. An attacker may alter the camera's images, change the view angle, or disable the UAeV's sensors and batteries. These attacks utilize malware or communication methods. An adversary's main aim is to modify or destroy network functioning intentionally. An attacker may then eavesdrop, modify, or erase data in transit. The increasing use of communication apps increases the attack surface. Thus, the wireless mesh networks or vehicular ad-hoc network-based attacks can be used against the UAeV communication system. Although the data connection appeals to attackers, the control link between the control system and the aircraft remains the primary target. Thus, using simple methods like jamming, spoofing, an attacker may successfully disrupt UAeV operations.

C. SOLUTIONS TO CHALLENGES USING BLOCKCHAIN TECHNOLOGY

In the blockchain, many challenges can be resolved [1]–[4]. Various possible solutions to existing challenges are briefly discussed as follows:

- **Protection from authenticated parties or insecure or untrusted networks**: In UAeV systems, blockchain technology helps establish a secure decentralized manner without using untrusted third parties. Thus, it helps establish a safe and trusted environment where data is distributed across the blockchain network and stored in off-chain records. All of these configurations build more trust and reliability over the existing network.
- **Collaborative and collective responsibility**: In a blockchain network, transactions are verified using majority-based verification and validation process. In these blockchain networks, 51% attack is standard, but maximum use of public-blockchain network can avoid this attack.
- **Data integrity and privacy concerns**: In UAeVs networks, data accuracy and consistency are significant concerns that lead to various cyber or GPs-based attacks. Therefore, blockchain is more appropriate to avoid attacks because it uses hash functions and public critical cryptography-based primitives. UAeV's information written in interconnected blocks and distributed in a decentralized network makes it difficult to delete or modify any of its parts or whole. Thus, this feature intrinsically ensures higher security to UAeVs and reduces the chances of failure to a large extent.
- **Authenticity**: It is possible to verify the data and user authenticity. In UAeVs, data authenticity is more important as compared to user authenticity. These procedures can be ensured using hash functions and digital signature approaches using in blockchain networks.
- **Identity and event management**: User identities and network events can easily be monitored and analyzed. As blockchain technology brings more transparency to network or user activities or transactions, it is possible to protect it from identity or unauthentic events.
- **The immutability of data records collected from users, UAeVs, and ground control systems** are easy to maintain an immutable database of events occurring from users, UAeVs, or ground control systems. In blockchain networks, the consensus among nodes is established using proper communications. Further, records are distributed across the nodes for maximum immutability. Integration of other systems (cloud servers) increases the scalability of the network. The presence of robust consensus and immutability property ensure data and network protection. This lead to a more trusted network as well.
- **Safe distance bounding mechanism**: In a blockchain integrated AVs network, all AVs are interconnected in a distributed ledger. This interconnection also ensures distance bounding, i.e., if any two autonomous vehicles want to communicate, they must like in one blockchain network with block's interconnectivity to update the information. In these interconnections, identities are hidden as well. Thus, a secure identity proof mechanism is possible through blockchain.
- **Blockchain properties**: There are three types of blockchain: private, public, and consortium-based. All of this blockchain provides and compared using different functionality. Centralization, transparency, traceability, mutability, data repudiation, scalability, adaptability, and permission or permissionless access are some of the key features. For example, a public blockchain provides decentralized, transparent, traceable, immutable, non-refusable, low scalable and flexible, and permissionless blockchain networks. Thus, public blockchain is more trustworthy compared to private or consortium-based approaches.

D. CASE STUDY 1: UNMANNED AERIAL VEHICLES, SENSORS, IoT, TELECOMMUNICATION NETWORKS AND BLOCKCHAIN

The massive growth of the IoT application areas has been associated with the technologies through efficient IIOT systems [240], [241]. The UAV-based applications are critical components of the IoT and sensor deployment in the air serving as an active platform. However, these applications have the pitfall of a vulnerable to a security attack [242]. As a result, the recent trend is to employ blockchain technology to reinforce the security of distributed storage through cryptographic approaches like hash functions. This technology is applied in the IoT-based application that utilizes next-generation wireless communication networking [243]. Hence, a case study demonstrates blockchain's development of a distributed storage model for UAVs-to-ground IoT networks [242]. This study emphasizes the importance of UAVs

equipped with AiS securely transmitting the sensed information from UAVs to GSM, as illustrated in Figure 19 and explained in the following steps [19].

Step 1:- The ASs gathers the data from the environment at different elevations.
Step 2:- The sensed data broadcasted to the Ground network, i.e., GSMs by the active ASs requesting storage space from the GSM because of the limitation of caching space.
Step 3:- The GSM provides the storage space for ASs as per the closest physical proximity responses.
Step 4:- The data sent from the UAV to the GS
Step 5:- After receiving the data, the GS verifies the successful reception of data and sends the acknowledgment to the UAV.
Step 6:- After receiving the acknowledgment from GS, the UAV assigns the reward points to GS through blockchain technologies such as smart contracts and the PoS consensus protocol.

The blockchain plays a vital role in this procedure because it enables secure data storage and communication between the UAVs and GSMs. Furthermore, the GS will receive blockchain rewards for providing services such as processing power and storage that allow the mutually beneficial model to function. Apart from these benefits, blockchain technology enables the following applications.

i. ***Enhances the data security:*** The UAVs cache the data from the environment and instantly transfer it to GSM by requesting caching space to secure their data. In return, UAVs awards the reward points to their traction through the blockchain. Hence, it mitigates the physical or cyber-attacks from adversaries because of the instant data transformation.
ii. ***Transactions between heterogeneous IoT sensors:*** This model provides mutual benefits to GSM and UAVs. Hence it creates a healthy heterogeneous environment.
iii. ***Inadequate processing power and storage:*** UAVs lack sufficient processing and storage power. Therefore, ASs sends the cached information quickly to GSM, which enables the capture with the next dataset and enhances the flying time through rescuing the data processing power.

XIII. ISSUES, CHALLENGES, DISCUSSIONS, AND FINDINGS

After analyzing different types of AVs, this section discusses the security issues, challenges in AVs and develops the discussions over them. Details are presented as follows.

A. SECURITY ISSUES AND COUNTERMEASURES USING BLOCKCHAIN IN AVs

The various security issues in autonomous vehicle systems and countermeasures using blockchain are discussed as follows [244].

- *User privacy*: The IoT network associated with any type of AVs share user information, including user location and identity, to track the user and vehicles in case of an accident. This information is important for concerned authorities to respond timely and correctly and regulate on-ground traffic conditions. On the other hand, sharing this information can lead to severe threats. For example, attackers or attackers may hack the system anonymously and escape by ascertaining a user's identity. Compared to other security approaches, blockchain maintains a high level of privacy by ensuring those nodes participate in the private blockchain network that is more trustworthy. In such cases, private blockchains are more secure compared to public or consortium-based blockchains. Further, consortium or hybrid blockchain can provide a provision to determine which data remain private and which data can be shared publicly in AVs networks.
- *Delay in response generation*: The present security frameworks fail in providing a real-time response in any type of AVs network. This is because of the use of resource-intensive processes. Using blockchain technology and a shared ledger of AVs, real-time responses or data can be fetched easily from sensors. These responses helps in operating the AVs efficiently.
- *Dynamic operating conditions*: Any type of AV is highly mobile. IoT networks or security frameworks designed for IoT-based applications are not useful because the parameters for security protocols keep changing. The roadside infrastructure is also unable to maintain a proper connection with vehicles. Blockchain ensure speed and scalability for security frameworks. It is possible to execute thousands of transactions in few milliseconds. All of these transactions follows logical rules to auto-fill the required information in AVs network. Thus, blockchain technology is capable of handling dynamic operating conditions of AVs.
- *Slow data validation*: AVs generate a lot of data that need to be collected, analyzed, and visualized at a much fast rate to ensure autonomous operations. Data verification and validation are also required to protect it against any attack. Lack of such verification or validation procedures can result in attacks to overtake the network traffic and generate unusual responses. Blockchain technology provides different provisions to verify and validate the data. For example, data registration, verification, and validation are possible using a blockchain network. All registered data can be linked to AV's hashchain, which in turn ensures data validation. In addition to data verification, node verification processes also exist in the blockchain network. These verification processes ensure data integrity and avoid any attacker's data as well.
- *Scalability*: As compared to other data-centric approaches, the blockchain-based data-centric distributed security approach is highly scalable. For example, the holochain approach is agent-centric, and it is

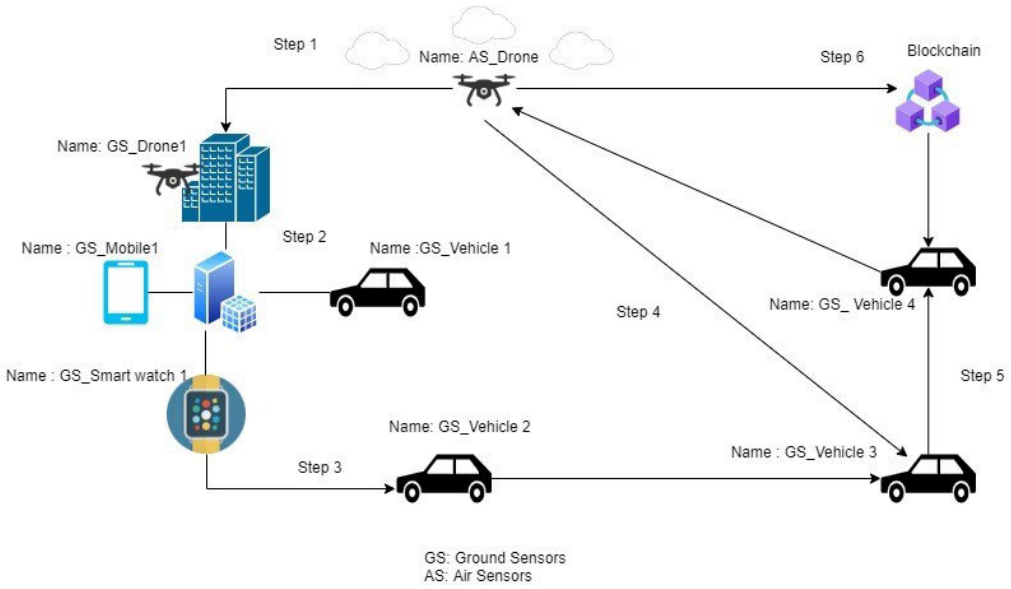


FIGURE 19. Decentralized storage system using UAeV, ad-hoc connectivity, IoT and blockchain.

highly scalable because of the independent participation of data encryption and storing it uniquely.

- *Congestion-based attacks*: Blockchain is a distributed solution to automotive security and privacy. Using blockchain, a large amount of data generated by AVs can be collected and processed in a distributed manner rather than centralized processing. Failure in centralized processing may result in device blockage or congestion inside the network. Thus, blockchain is a much efficient approach compared to centralized processing infrastructure.
- *Connectivity*: Blockchain-based consensus protocol provide better connectivity with low communication complexity, minimum delays, low energy consumption, and resistance against attacks. These protocols can also be customized to handle fast error detection and correction, fault tolerance, scalability, and integrity issues.
- *Other issues and solutions using blockchain*: Other issues and solutions include: (i) Blockchain ensure immutability which inturns make user accountability, irrevocable transactions, transaction integrity, tamper-proof records (user and vehicle), data verifiability and authentication, (ii) Blockchain can provide interconnection more flexibly with secure transactions using smart contracts, multiple consensus algorithms, and dynamic and heterogeneous nodes, and (iii) Decentralized approach of blockchain avoid single point of failure, lesser transaction fees, more trustworthy and efficient computational environment.

B. SECURITY ISSUES AND COUNTERMEASURES USING BLOCKCHAIN IN VEHICULAR NETWORKS

The various security issues in vehicular networks and countermeasures using blockchain are discussed as follows [245]–[253].

- Khelifi *et al.* [245] discussed the one of the most intriguing aspects of Named Data Networking (NDN), a possible future Internet architecture based on content names rather than host addresses, is the ability to cache information inside the network. NDN has had many difficulties since it was originally deployed in vehicular ad-hoc networks (VANET), including issues with security and trust, to name a few. In this work, reputation-based methods is used to enhance trust in vehicle caching settings. This work can be extended to generate and evaluate reputation scores that can effectively avoid attacks.
- Li *et al.* [246] discussed that vehicular network faces challenges in security and privacy areas at multiple fronts. For example, privacy leakage is a major concern. In this, important user or vehicle information is insecurely disseminated to others, leading to an unfair ''free-riding'' issue. To avoid such security and privacy concerns, the proposed approach uses blockchain and Merkle hash tree to ensure a concrete, fair and anonymous approach that avoids ''free-riding'' attacks. The importance of smart contracts is considered to disseminate reward-based mechanisms for ethically performing the disseminating task. In analysis, it has been observed that the proposed approach is effective in terms of anonymity and conditional linkability. The computation, communication, and delay analysis show that the proposed approach effectively ensures security for vehicular networks. This work can be extended to include other blockchain and vehicular network-based performance parameters to ensure its all-around performances in vehicular communication. For example, transaction response time, end-to-end delay, transaction fee variation, and network throughput are some of the important and interesting parameters to explore.

- Shrestha and Nam [247] discussed that blockchain technology could provide a realistic solution to the issues of sending safe communications and preserving data in automotive networks. This work has explored the architecture of a regional blockchain to help with the development of VANETs, in which all nodes are grouped together within a particular geographic area. Security issues of this area are considered for analysis. This work has explored how to create a blockchain that covers a region while minimizing the possibility of a 51 percent attack to secure this area. Further, work can be extended to discuss the issues with the regional blockchain network. For example, scalability is a major concern in the blockchain. Thus, analysis of scalability of the network, chances of immutability attack and performance issues can be interrelated and explored in detail.
- Yang *et al.* [248] discussed that information on traffic safety and fuel efficiency is transmitted and disseminated by cars to make transportation more convenient. Vehicles face various security challenges in vehicular networks. For example, vehicles have a tough time evaluating the authenticity of incoming signal signals because of the poor security environment. Blockchain technology is used to build a decentralized trust management system for vehicle networks, as suggested in this study. A decentralized system with consensus in the network can secure the vehicular network. In the proposed system, each vehicle uses a Bayesian Inference Model to verify that a signal from another vehicle is genuine. Thus, it ensures security from multiple fronts. In the future, the use of trust management and security preservation can be explored in detail.

Table 14 shows a comparative analysis of recent literature over the blockchain-integrated vehicular network. Among other related work [249]–[253], the importance of blockchain in the vehicular network is explored. For example, In [250], various attacks in blockchain-integrated applications are discussed. These attacks can be explored for the vehicular network as well. Guo *et al.* [252] discussed the trust management-based approach to ensure high reputation blockchain-based vehicular network. This can avoid attacks using trust management in the trusted network. Figure 20 shows the eight blockchain technology integrated concerns (including security issues) that need in-depth attention in the near future for vehicular networks.

C. BLOCKCHAIN-INTEGRATED TRUST MANAGEMENT SCHEME FOR VEHICULAR NETWORKS

Recent blockchain-integrated trust management schemes for vehicular networks are briefly discussed as follows [248], [255]–[259].

- Khelifi *et al.* [245] discussed that a reputation-based approach for implementing trust and securing caching in a vehicular network context is useful in avoiding various attacks. The proposed system is built on the blockchain network and incorporates caches, each of which has a reputation value that changes depending on the materials that have been supplied. This investigation concluded that cached and served data alone should include secure information, disregarding anything else. This work can be extended to propose multi-constraint trust computation approaches for multi-objective function design.
- Lu *et al.* [254] explored a trust-management-based reputation model for the vehicular network. Although PKI-based authentication offers just the absolute minimum in security features, vehicle ad-hoc networks often utilize it. To build trust, this work put in place a trust model for the sender. The proposed model rely on both our past encounters and indirect perceptions of the sender in order to compute trust and achieve a secure vehicular network. Distributed trust management may be implemented with vehicle' privacy intact when the proposed model (named as blockchain-based anonymous reputation system (BARS)) is capable of doing so. This work performed delay-based authentication analysis in performance measurement. However, this work can be extended to include other performance parameters for evaluation—for example, trust generation, propagation, collection and regeneration delays. Similarly, network throughput, jitter, end-to-end delays, system training time, and trust score variation are some of the other parameters to focus upon.
- Yang *et al.* [248] proposed blockchain-based decentralized trust management approach for vehicular networks. To increase overall traffic safety and efficiency, vehicles communicate with one another. AVs can't adequately judge the reliability of incoming signals because of the constantly changing environment in which they operate. Trust management can help every entity in the vehicular network rely on other nearby entities for decision-making. A trust management system for automobile networks, implemented using blockchain technology, is described in this work. In order to verify the signals it has received from nearby cars, each vehicle is proposed to use a Bayesian Inference Model. This work has listed various attacks. However, a formal security analysis can be performed to measure the security level.
- Javaid *et al.* [255] discussed that intelligent vehicles and intelligent transportation systems can be integrated via an IoT-based system. Intelligent transportation systems depend on vehicle-to-vehicle (V2V) communications and constitute vehicular ad-hoc networks. It is critical that intelligent vehicles communicate reliably and securely both inside and across their network (provenance). This work describes a system architecture for trusted and intelligent vehicle registration that uses blockchain technology and a certificate authority. Here, a proposal is made to establish secure communication between vehicle to vehicle and vehicle to roadside unit. However, the performance or security analysis of the proposed approach lacks in this work. Thus, this

TABLE 13. Comparative analysis of recent studies on blockchain and UAeV.

Author	Year	A	B	C	D	E	F	Major Findings	Major Shortcomings and Challenges
Tejasvi Alladi et al. [19]	2020	×	✓	✓	×	×	✓	Open challenges, future directions and blockchain integrated UAeV applications and solutions.	Design issues on Blockchain integration with AUV not discussed.
Rani. C et al. [235]	2016	×	×	✓	✓	×	×	Isssues of cyber attcks and security issues of blockchain enabled UAeV. Hacking mechanism demonstrated over UAeV.	Cryptographic techniques and Encryption mechanisms not detailed as solution to security issues.
Álvares, P et al. [236]	2021	×	✓	✓	✓	✓	✓	Detailed review on blockchain enabled connected UAeV solutions, challenges and research directions.	Recommendations of blockchain solutions in smart city environment discussed. However issues around their security and vulnerability not discussed.
M. Aloqaily, et al. [237]	2021	×	×	✓	✓	✓	✓	Integration of 5G and fog/MEC computing in blockchain enabled UAeV solutions for high data rates.	In 5G and fog / MEC integrated blockchain solutions especially in case of connected UAeV, security issues and recommendations not discussed.
Alsamhi, S.H. et al. [238]	2021	×	✓	×	✓	✓	✓	Blockchain enabled UAeV solutions to combat Covid-19 pandemic and further pandemics.	Design issues not discussed. Security issues outline however its impact on various use cases not detailed.
Santos De Campos et al. [239]	2021	×	×	✓	×	✓	✓	Multi-UAeV surveillance framework discussed.	This work is focused towards application of multi-UAeV in monitoring and surveillance use cases. Issues related to network (speed of message delivery) not discussed.

A: Short survey, B: Long and in-depth survey or analysis, C: Blockchain integration issues D: UAeV Network and security issues , E: Multi-UAeV issues, F: Blockchain enabled UAeV applications.

TABLE 14. Comparative analysis of recent literature over the blockchain-integrated vehicular network.

Author	Year	A	B	C	D	Issues in Traditional Vehicular Network	Blockchain-based Solution	Future Directions
Khelifi et al. [245]	2018	✓	×	✓	✓	Discussed the importance of securing in-network caching to avoid various attacks, including DoS, wormhole, replay etc.	A reputation-based mechanism is proposed in this work to avoid attacks. A reputation value to each cache source is assigned and varied based on its performance.	This work can be extended to generate a reputation matrix for statistical reputation score generation and usage for avoiding attacks.
Li et al. [246]	2019	×	✓	✓	×	Discussed the "free-riding" attack raises due to security and privacy concerns in a vehicular network.	Proposed blockchain and Merkle hash tree-based reputation scheme to avoid "free-riding" attack and protect the user and vehicle's unethical data dissemination.	This work can be extended to include more performance-based parameters to measure and evaluate the performance in detail of the proposed scheme.
Shrestha and Nam [247]	2019	✓	✓	×	×	This work has explored the situations that can be used for mitigating immutability attacks in vehicular networks. Immutability attack-associated parameters are explored to ensure stable operations in vehicular networks.	Regional blockchain is formulated for the vehicular network to avoid attacks. Analysis of blockchain-based solutions is discussed in detail.	This work can be extended to include blockchain-based issues in handling immutability attacks in a more extensive network. For example, scalability and its impact on regional blockchain performance can be explored.
Yang et al. [248]	2019	✓	✓	✓	×	This work has considered message credibility into its centric area to secure and explore using blockchain technology. Use of road-side units is necessary to explore because there are computational and security issues in these devices.	Blockchain-based message credibility evaluation is discussed in this work. Additionally, the trust management approach is applied with the help of road-side-units to create a reliable and consistent trust blockchain.	In the future, joint integration of trust management and privacy preservations can be explored to ensure a reliable decentralized trust framework for the vehicular network. This can ensure a safe and efficient transportation system.
Dibaei et al. [249]	2021	✓	✓	✓	×	This is an extensive survey over-analyzing cyber-attacks and providing countermeasures to avoid them using blockchain and machine learning concepts. This work has discussed the important security issues including, secure data storage, transmission, accessibility, contribution, and sharing. These issues may arise from road-side units, users, networks, devices or vehicles,	This work has conducted an in-depth survey over strengths, limitations, and future directions of recent blockchain and machine learning-based approaches proposed to avoid data security at every point. Further, blockchain-associated concepts and their importance to vehicular networks is explored.	This work can be extended to include blockchain-based issues for vehicular networks. For example, scalability with an increase in vehicles and data is a major concern to address and evaluate in detail with computational and communicational cost perspectives.

A: Cyber or physical attacks over roadside units of vehicular infrastructure, B: Cyber-attacks over vehicles in vehicular networks, C: Data-security issues in vehicular networks, D: routing or caching issues in vehicular network's infrastructure.

work can be extended to include formal security and attack analysis, and QoS-based network performance measurements.

- Liu *et al.* [256] discussed the use of anonymous aggregate vehicular announcement protocol. Users may choose to utilize the proposed protocol, which enables

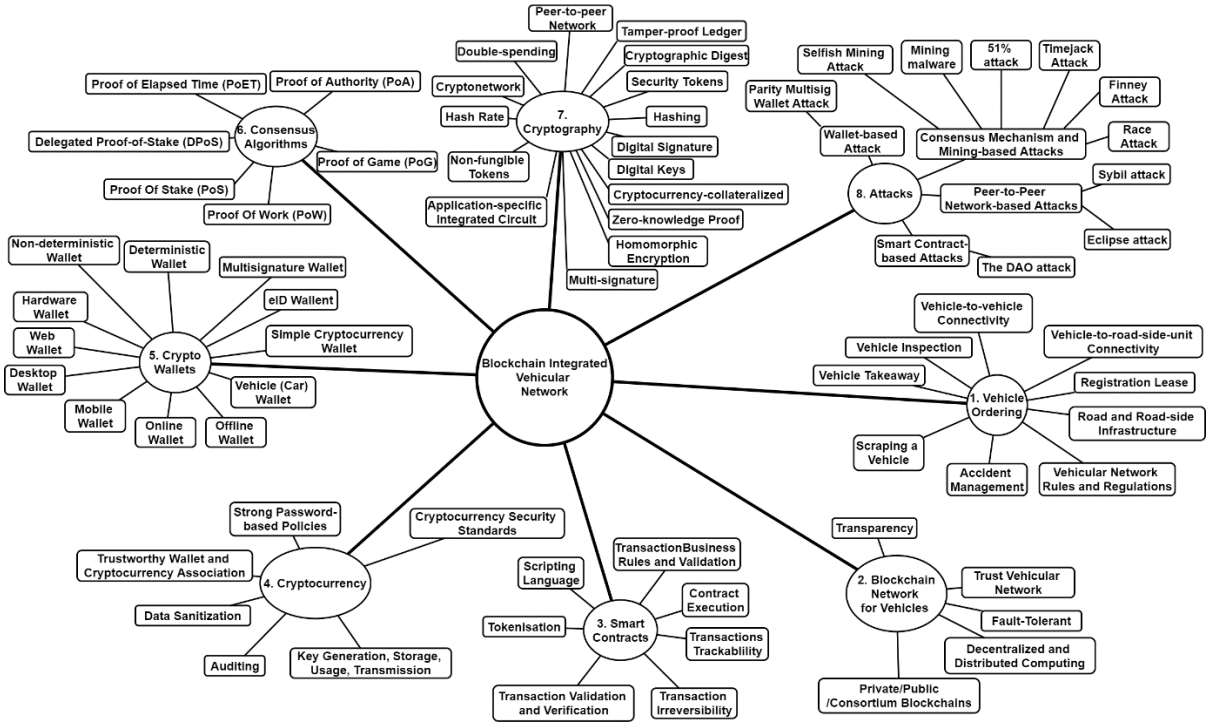


FIGURE 20. Eight important concepts to learn and explore for blockchain-integrated vehicular network.

vehicles to send messages anonymously to preserve the privacy of their discussion. Roadside units use vehicle reputation values to evaluate message dependability. These values are safely kept on the blockchain and are computed by roadside units, and they are used to determine message dependability. The use of trust ratings in conjunction with logistic regression may help to improve the accuracy of the detection of hostile vehicles even more. This work has performed performance analysis using various trust-based parameters and mentioned few attacks. However, the formal security analysis of the proposed approach is lacking in the present work. Thus, this work can be extended to analyze the attack scenarios and possibilities formally.

Table 15 shows a comparative analysis of recent literature over trust management approaches in blockchain integrated vehicular network. Among other approaches [257]–[259], blockchain and trust management approaches are discussed to secure user or vehicle location, information, data exchange methods, or communication medium. In addition to creating a blockchain network, these approaches focused on other blockchain-associated concepts, including smart contracts to payoff for trusted services, cryptocurrencies, and wallets for digital transactions, and miner approaches to generate challenges for all types of users (authorized or unauthorized). All of these concepts generate a trusted information exchange network for vehicular networks. Figure 21 shows the blockchain technology integrated trust management concepts (including security issues) that need in-depth attention in the near future for vehicular networks.

D. CHALLENGES

The various challenges in blockchain-based autonomous vehicle systems are briefly explained as follows [10].

- *Lack of sophisticated mobility model*: It has been observed that wireless connectivity-based autonomous vehicle systems lack track channel errors. These systems apply approximation approaches in specifying the characteristics of AVs. As a result, it requires advanced time-varying channel models in conjunction with vehicle mobility to track the evolution of the channel state as each vehicle moves.
- *Lack of mobility-aware efficient verification*: In autonomous vehicle networks, vehicle movements are highly mobile. Thus, issues concerning blockchain network performance arise. Therefore, there is a lack of a blockchain technology framework for a mobile environment suitable to autonomous vehicle networks.
- *Lack of specific blockchain technology solutions*: The existing studies integrating blockchain technology with AVs are very generic. They discuss the importance of private, public, and consortium-based blockchain for AVs. However, there is a lack of discussions over autonomous vehicle's feature-based blockchain networks to improve user experiences and infrastructure requirements.
- *Wide adaptability and performance concerns*: In this study, it has been observed that there are various types of AVs. All of these vehicles have their usages in a different set of applications. AVs with similar features but

TABLE 15. Comparative analysis of recent literature over trust management approaches in blockchain integrated vehicular network.

Author	Year	A	B	C	D	E	Issues in Traditional Vehicular Network	Blockchain-based Solution	Future Directions
Khelifi et al. [245]	2018	✓	×	✓	✓	I	Discussed that securing the caching resources in the network is important to avoid any type of attack and increase trust and performance.	The proposed system is built on the blockchain network and incorporates caches, each of which has a reputation value that changes depending on the materials that have been supplied.	This work can be extended to propose multi-constraint trust computation approaches for multi-objective function design.
Lu et al. [248]	2018	✓	✓	✓	✓	I	Trust and privacy among any two enetities in vehicular network is an important concern. To ensure autonomous vehicle movements, this is necessary for smooth operations.	The proposed model relies on both past encounters and indirect perceptions of the sender to compute trust and achieve a trusted blockchain and secure vehicular network.	Performance analysis of proposed work is limited to authentication delay calculation. Other performance parameters can be taken for evaluation.
Yang et al. [254]	2019	✓	✓	✓	✓	I	Trust preservation and privacy are major concerns for AVs and vehicular networks. Attacks (e.g. bad-mouthing, ballot) over trust-based reputation systems are observed in recent studies.	Trusted blockchain and trust management can ensure entity-to-entity rely on decision making. Here, an entity could be a vehicle, user, roadside unit, or any equipment in vehicular infrastructure.	This work can be extended to formally analyze the security attacks. Further, lightweight characteristics of the proposed model can be identified to make it feasible for resource-constraint devices in vehicular networks.
Javaid et al. [255]	2019	✓	✓	✓	✓	S	Traditional vehicular network lacks in building efficient centralized computing infrastructure for roadside units or vehicular networks	Blockchain and trust management can provide a distributed, decentralized, and secure computing infrastructure for vehicular or roadside unit infrastructure.	This is a conceptual work and can be extended to perform formal security and performance analysis of proposed algorithms.
Liu et al. [256]	2020	✓	✓	✓	×	I	Sending broadcast messages across vehicular infrastructure may create many security and performance issues.	Users may choose to utilize the proposed blockchain-based protocol, which enables vehicles to send messages anonymously to preserve the privacy of their discussion.	This work lacks in a security analysis of the proposed approach. The attack scenarios and security level can be estimated for the proposed scheme.

A: Trust management, B: Trust-based reputation score for network entities, C: Performance analysis, D: Formal security and/or attack analysis, E: Survey (S)/Implementation (I)-based article.

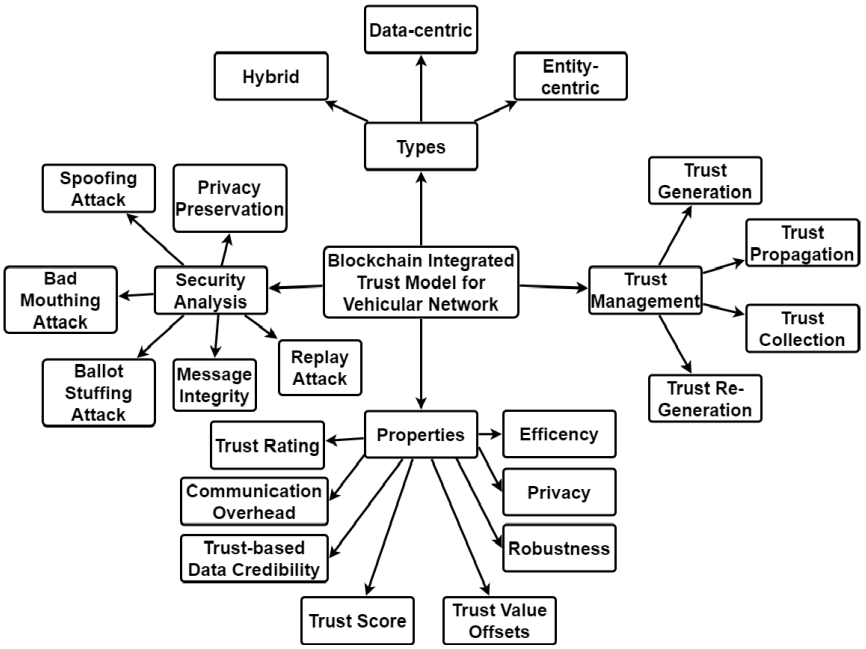


FIGURE 21. Important concepts to learn and explore for blockchain-integrated trust management for vehicular network.

other operations encourage to development of a common framework that ensures an automation-controlled system for vehicles with maximum safety and better performance.

- *Multi-purpose smart contracts*: As discussed earlier, the industry needs multiple-purpose intelligent contracts to handle numerous financial stakeholders. Likewise, smart contracts with blockchain technology can handle various other AVs and their infrastructure operations. Presently, there is a lack of similar studies, designs, implementations, and discussions.
- *Muddle Mixture of human or robot responsibilities*: As discussed earlier, various AV accidents and attacks over their infrastructure are observed in recent times. In the present scenario, humans are involved in backup systems, which is one of the significant drawbacks. In case of accidents, responsibility has to be fixed, which is not because it is pretty challenging to decide who is responsible, a human or machine. Thus, regulatory moves are required with the support of blockchain technology to ensure permissible evidence. In this work, we started by comparing the recent blockchain-based autonomous vehicle studies and surveys. After that, three types of AVs (AEV, AGV, and AUV) and their associated parameters are considered for in-depth analysis and association with blockchain concepts. The other on-road AVs are addressed in the 'autonomous vehicle' category only. In this work, discussions are developed over the vehicle's features, followed by how these features can be associated with blockchain concepts for improving the on-road experiences.

XIV. CONCLUSION, LIMITATIONS, AND FUTURE DIRECTIONS

Blockchain transforms autonomous systems and vehicles like other industries (e.g., healthcare, supply chain, insurance, music, and many more). Blockchain is applied to power AVs and improving customer retention, satisfaction, trust, and other experiences. Blockchain is considered for secure vehicle data management, storing, transferring, and sharing in autonomous systems. The data includes vehicle identification, its wear and tear, insurance, loans, user experiences, mileage, and many more. This work will help the readers understand the recent trends in AVs and acquire knowledge of different AVs, their features, and future directions to integrate smart contracts, cryptocurrencies, blockchain networks, and distributed ledger with advanced blockchain concepts wallets.

Further, gaining knowledge in the diversity of existing blockchain-based autonomous studies and their comparative analysis helps identify innovative practices, challenges, and possible solutions. Finally, use-cases are taken up by an author (with industry background) to give examples and the importance of blockchain in AVs. These use-cases help in the identification of parameters used to measure the performance and cost of AVs. Overall, performance is observed to be better with less cost compared to manual processes. Many limitations, research directions, and solutions are still needed to be explored that have been missed in this work. Some of these limitations and future orders are elaborated as follows.

A. LIMITATIONS

This sub-section presents some of the limitations of this and existing works. Details are explained as follows.

- *Lack of smart contract-based smart and secure data handling in an autonomous vehicle:* The present survey does not discuss the smart contract-based frameworks or methodology to control autonomous vehicle movements. The existing work generalizes the discussions over smart contract usages and advantages rather than focusing on integration and performance analysis. Further, there is a need to design and analyze smart contracts for different types of AVs.
- *Vehicle's internal parameters for blockchain network:* With the blockchain integration with the autonomous vehicle network, there is a need to identify those vehicle parameters to improve user experience and make an error, attack, and accident-free vehicle movement. These parameters may vary according to the type of autonomous vehicle. For example, the performance and cost of the AGV are identified in this work for designing smart maintenance contracts. Likewise, other parameters for different vehicles can be specified to create a vehicle's blockchain network.
- *Vehicle's external parameters for blockchain network:* there is a lack of infrastructure requirement understanding for AVs. Various proposed are made to integrate advanced technologies (IoT, Cloud, future generation networks) with AVs and systems. Now, what parameters from these technologies will be helpful to create a blockchain network and why? It is an open-addressed challenge that needs attention.
- *Massive storage requirements:* The existing work discusses proposals to handle storage requirements by integrating promising technologies like 5G, edge computing, cloud computing, and ML-based systems. With the increase in V2X connectivity and autonomous vehicle scalability, the challenges to store a large amount of data, data management, V2V transactions, and data security increase. Thus, there is a lack of discussions over how blockchain technology will work in computationally high requirement-based infrastructure.
- *Lack of use cases:* Presently, this work is performed to design use-cases for automated guided vehicles. However, the use-cases are developed for other types of AVs. These use-cases can help in identifying the challenges and possible solutions. After that, it can be used in simulation followed by successful implementation.
- *Improved QoS for AVs:* Various cyber threats and cyber-attacks are observed over autonomous systems in recent studies. Dreadful QoS of an autonomous system is a significant cause. Thus, there is a need to explore improving QoS for autonomous systems and associated infrastructure.
- *Other limitations:* autonomous vehicle coordination, data security and privacy, lightweight cryptography

primitives and protocol identification, laws, standards and procedures to operate, storage systems, fuel and energy backups, and cost are other important limitations that need to be addressed before accepting AVs on roads and streets.

B. FUTURE DIRECTIONS AND POSSIBLE SOLUTIONS

In the future, in the following directions and possible solutions, this work can be extended:

- Explore more effective green energy solutions and energy backup systems for AVs. For example, there are multiple green energy solutions like solar power, wind power, hydropower, geothermal energy, biomass, and biofuels. These green energy solutions have their own set of energy production, storage, and distribution strategies. Thus, there is a need to explore these green energy solutions and the role of blockchain technology in energy production to the consumption cycle. For example, Teng *et al.* [260] discussed that the lack of a proper management platform for vehicular network computing is a significant constraint on the development of the system, which has been a hindrance to its maturity for a long time. The proposed approach uses the green energy consumption as well as the communication latency between jobs and block creation as part of an integrated optimization strategy to increase efficiency to the greatest extent. Likewise, green energy solutions and system performance can be integrated for AVs and vehicular networks to improve efficiency and reducing the present and futuristic costs.
- Smart contract features can be surveyed for AVs. After that, a smart contract can be designed, developed, and tested for performance measurements and evaluations. A smart contract integrate every user or system with a digital contract. With an event-based monitoring network, a smart contract can execute the transactions. Thus, the autonomous processes are much faster, responsible, and accountable. A smart contract also stores every event in a memory location for evaluation. Thus, the design, implementation, evaluation, and analysis of smart contracts will be helpful to explore and extend for autonomous vehicles and systems. For example, In [215], [255], [258], smart contracts are discussed with respect to trust management approaches for blockchain-integrated vehicular networks. In these smart contract-based approaches, the reputation of the vehicular network is build using trust management. Smart contract executes along with some transactions when the trust management system responds with a good reputation rating. Thus, smart contracts are associated with a reputation system, trust rating, blockchain, and vehicular networks to improve system efficiency and reliability.
- Blockchain technology is proposed for AVs through different means. However, exploring the cryptographic primitives and protocols for blockchain technology-integrated AVs is yet to study. For example, there is the use of various types of sensors in AVs, as discussed before. These sensors are lightweight and have a scarcity of resources. Thus, The lightweight cryptographic primitives and AV protocols are investigated for computational and communicational costs with the existing cryptographic techniques. A comparative analysis of lightweight primitives and protocols using computational and communicational costs will help identify a range of mechanisms that can be used for resource constraint devices to resourceful devices associated with the blockchain network. For example, In [261]–[264], various lightweight solutions are proposed to ensure cryptography services like authentication, encryption/decryption, and primitives processing. Likewise, solutions are proposed to provide lightweight but secure connectivity between vehicles or vehicles and roadside infrastructure. Here, infrastructure may include cloud infrastructure for distributed processing for AVs and vehicular networks. The cloud infrastructure.
- In the future, studies on QoS and its improvements can be conducted for different types of AVs. These studies should discuss the performance aspect in-depth without compromising on security aspects. For example, what consensus algorithm will give a secure and real-time response to various autonomous vehicles? What would be the variation in renewable energy utilization rate, number of blocks with different capacities, information sharing mechanism in multi-chain structure, and QoS score with the integration of blockchain technology? Likewise, other parameters, including block frequency, block size, workload type, node configuration, network size, network structure, workload quality, miner and mining details, and programmable application interfaces can be designed and standardized for autonomous vehicles and systems. In [248]–[259], the majority of contributions performed limited performance or security analysis. These contributions can be extended to include performance and security parameters, including attack analysis (bad-mouthing, ballot stuffing, replay, DoS etc.). Similarly, performance parameters important to analyze include trust score variation with time, network device's reputation and response time, the smart contract execution time for vehicular networks etc. Thus, performance parameters are important to explore.
- The existing survey can be extended to have in-depth studies over vulnerabilities, attacks, loopholes, and countermeasures for autonomous vehicle infrastructure. The present surveys focus more on autonomous vehicle performances and coordination. The existing work can be extended to have an in-depth analysis of blockchain-integrated autonomous vehicles and systems. In addition, surveys can be used to investigate consensus processes, smart contract designs, blockchain network types, web, mobile, or hardware wallets, and

applications for autonomous vehicles. In this work, security attacks and blockchain concepts are important to understand for blockchain-based vehicular networks and trust-management-based vehicular networks. However, the key terms used in deriving these hierarchies can be mathematically analyzed and surveyed in-depth.

- More use-cases can be designed to identify the features and implementation issues for different types of AVs. For example, there are multiple autonomous vehicles and systems, including AUV, AAeV, AEV, and UUAV. All of these have a different set of functionalities and usages for various applications. Thus, exploring the uses of each of these autonomous vehicles, associated mathematical models, pros, and cons would be attractive. Here, formal security-based mathematical models are widely discussed in recent studies. These models help in understanding the attack scenarios and perform security countermeasures. Likewise, mathematical models and associated uses can be explored for highly dynamic connectivity concerns in vehicular networks. Integrating security models, trust management, blockchain concepts, and vehicular network connectivity and communication require formal analysis. This is possible with a mathematical model only. Thus, the importance of these models and variations among different types of AVs is important.
- This work discusses the vehicular network briefly. Integration of ad-hoc connectivity-based vehicular networks using UAeVs is another important domain to explore in detail. Examine the security challenges that come with vehicle networks and the potential significance of the blockchain. For example, In [248]–[259], this work explores vehicular networks. These vehicular networks and the importance of blockchain are discussed in detail. However, comparative analysis of security models concerning security properties is important to realize for vehicular networks. In this work, a comparative analysis of few security properties is done. However, this comparative analysis can be extended to analyze the lightweight security aspects for heterogeneous networks consisting of resourceful and resource-constraint devices used to operate the vehicular network. Additionally, trust score variation is high in dynamic networks. The study to extend the similar dynamic situations for vehicular networks are yet needs to be examined.
- Trust management is another important aspect in the constellation of AVs, users, and networks. In trust management, trust generation, propagation, distribution, and accumulation issues can be studied in the future. For example, In [255]–[259], various trust management approaches are proposed to build trusted blockchain and vehicular networks. In these approaches, trust rating models are discussed, using trust management phases to compute trust scores. This trust score is valuable to rate any vehicle's or infrastructure equipment performance. In blockchain integrated solutions, privacy and trust among vehicular network entities are built using this trust score, which further allows blockchain technology to execute the smart contract and perform transactions.

REFERENCES

[1] K. Wiggers. (Oct. 2020). *Waymo's Driverless Cars Were Involved in 18 Accidents Over 20 Months*. Accessed: Jun. 9, 2021. [Online]. Available: https://venturebeat.com/2020/10/30/waymos-driverless-cars-were-involved-in-18-accidents-over-20-month/
[2] J. Huang, L. Kong, G. Chen, M.-Y. Wu, X. Liu, and P. Zeng, "Towards secure industrial IoT: Blockchain system with credit-based consensus mechanism," *IEEE Trans. Ind. Informat.*, vol. 15, no. 6, pp. 3680–3689, Jun. 2019.
[3] F. Jahan, W. Sun, Q. Niyaz, and M. Alam, "Security modeling of autonomous systems: A survey," *ACM Comput. Surv.*, vol. 52, no. 5, pp. 1–34, Oct. 2019.
[4] G. Rathee, A. Sharma, R. Iqbal, M. Aloqaily, N. Jaglan, and R. Kumar, "A blockchain framework for securing connected and autonomous vehicles," *Sensors*, vol. 19, no. 14, p. 3165, Jul. 2019.
[5] J. Grewal. (Apr. 27, 2020). *Blockchain-Powered Autonomous Automobiles Can be the Answer*. Accessed: May 4, 2021. [Online]. Available: https://www.ibm.com/blogs/blockchain/2020/04/blockchain-powered-autonomous-automobiles-can-be-the-answer
[6] A. Kumar and S. Jain, "Proof of game (PoG): A game theory based consensus model," in *Sustainable Communication Networks and Application*. Cham, Switzerland: Springer, 2020, pp. 755–764.
[7] M. Pilkington, *Blockchain Technology: Principles and Applications*. Cheltenham, U.K.: Edward Elgar Publishing, 2016.
[8] *Bitcoin*. Accessed: Apr. 17, 2021. [Online]. Available: https://bitcoin
[9] R. Shivers, M. A. Rahman, and H. Shahriar, "Toward a secure and decentralized blockchain-based ride-hailing platform for autonomous vehicles," 2019, vol. 68, no. 8, pp. 4734–4746, *arXiv:1910.00715*. [Online]. Available: http://arxiv.org/abs/1910.00715
[10] S. R. Pokhrel and J. Choi, "Federated learning with blockchain for autonomous vehicles: Analysis and design challenges," *IEEE Trans. Commun.*, vol. 68, no. 8, pp. 4734–4746, Aug. 2020.
[11] M. Baza, M. Nabil, N. Lasla, K. Fidan, M. Mahmoud, and M. Abdallah, "Blockchain-based firmware update scheme tailored for autonomous vehicles," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, Apr. 2019, pp. 1–7.
[12] R. Shrestha, S. Y. Nam, R. Bajracharya, and S. Kim, "Evolution of V2X communication and integration of blockchain for security enhancements," *Electronics*, vol. 9, no. 9, p. 1338, Aug. 2020.
[13] H. Guo, E. Meamari, and C.-C. Shen, "Blockchain-inspired event recording system for autonomous vehicles," in *Proc. 1st IEEE Int. Conf. Hot Inf.-Centric Netw. (HotICN)*, Aug. 2018, pp. 218–222.
[14] X. Jiang, F. R. Yu, T. Song, and V. C. M. Leung, "Intelligent resource allocation for video analytics in blockchain-enabled internet of autonomous vehicles with edge computing," *IEEE Internet Things J.*, early access, Sep. 24, 2020, doi: 10.1109/JIOT.2020.3026354.
[15] S. Ayvaz and S. C. Cetin, "Witness of things: Blockchain-based distributed decision record-keeping system for autonomous vehicles," *Int. J. Intell. Unmanned Syst.*, vol. 7, no. 2, pp. 72–87, Apr. 2019.
[16] Y. Wang, Z. Su, K. Zhang, and A. Benslimane, "Challenges and solutions in autonomous driving: A blockchain approach," *IEEE Netw.*, vol. 34, no. 4, pp. 218–226, Jul. 2020.
[17] X. Jiang, F. R. Yu, T. Song, Z. Ma, Y. Song, and D. Zhu, "Blockchain-enabled cross-domain object detection for autonomous driving: A model sharing approach," *IEEE Internet Things J.*, vol. 7, no. 5, pp. 3681–3692, May 2020.
[18] A. Saini, S. Sharma, P. Jain, V. Sharma, and A. K. Khandelwal, "A secure priority vehicle movement based on blockchain technology in connected vehicles," in *Proc. 12th Int. Conf. Secur. Inf. Netw. (SIN)*, 2019, pp. 1–8.
[19] T. Alladi, V. Chamola, N. Sahu, and M. Guizani, "Applications of blockchain in unmanned aerial vehicles: A review," *Veh. Commun.*, vol. 23, Jun. 2020, Art. no. 100249.
[20] S. Megha, H. Salem, E. Ayan, and M. Mazzara, "A survey of blockchain solutions for autonomous vehicles ecosystems," *J. Phys., Conf. Ser.*, vol. 1694, no. 1, p. 12024, 2020.
[21] Y. Fu, F. R. Yu, C. Li, T. H. Luan, and Y. Zhang, "Vehicular blockchain-based collective learning for connected and autonomous vehicles," *IEEE Wireless Commun.*, vol. 27, no. 2, pp. 197–203, Apr. 2020.

[22] S. Mariani, G. Cabri, and F. Zambonelli, "Coordination of autonomous vehicles: Taxonomy and survey," *ACM Comput. Surv.*, vol. 54, no. 1, pp. 1–33, Apr. 2021.

[23] Y. Yang, Y. Xiao, and T. Li, "A survey of autonomous underwater vehicle formation: Performance, formation control, and communication capability," *IEEE Commun. Surveys Tuts.*, vol. 23, no. 2, pp. 815–841, 2nd Quart., 2021, doi: 10.1109/COMST.2021.3059998.

[24] A. M. Yazdani, K. Sammut, O. Yakimenko, and A. Lammas, "A survey of underwater docking guidance systems," *Robot. Auton. Syst.*, vol. 124, Feb. 2020, Art. no. 103382.

[25] P. J. B. Sánchez, M. Papaelias, and F. P. G. Márquez, "Autonomous underwater vehicles: Instrumentation and measurements," *IEEE Instrum. Meas. Mag.*, vol. 23, no. 2, pp. 105–114, Apr. 2020, doi: 10.1109/MIM.2020.9062680.

[26] J. Yuh, "Design and control of autonomous underwater robots: A survey," *Auton. Robots*, vol. 8, no. 1, pp. 7–24, 2000.

[27] S. Yoon and C. Qiao, "Cooperative search and survey using autonomous underwater vehicles (AUVs)," *IEEE Trans. Parallel Distrib. Syst.*, vol. 22, no. 3, pp. 364–379, Mar. 2011, doi: 10.1109/TPDS.2010.88.

[28] S. Williams, O. Pizarro, M. Jakuba, C. Johnson, N. Barrett, R. Babcock, G. Kendrick, P. Steinberg, A. Heyward, P. Doherty, I. Mahon, M. Johnson-Roberson, D. Steinberg, and A. Friedman, "Monitoring of benthic reference sites: Using an autonomous underwater vehicle," *IEEE Robot. Autom. Mag.*, vol. 19, no. 1, pp. 73–84, Mar. 2012, doi: 10.1109/MRA.2011.2181772.

[29] G. Antonelli, S. Chiaverini, R. Finotello, and R. Schiavon, "Real-time path planning and obstacle avoidance for RAIS: An autonomous underwater vehicle," *IEEE J. Ocean. Eng.*, vol. 26, no. 2, pp. 216–227, Apr. 2001, doi: 10.1109/48.922788.

[30] J. Melo and A. Matos, "Survey on advances on terrain based navigation for autonomous underwater vehicles," *Ocean Eng.*, vol. 139, pp. 250–264, Jul. 2017.

[31] C. Fang and S. Anstee, "Coverage path planning for harbour seabed surveys using an autonomous underwater vehicle," in *Proc. IEEE OCEANS*, May 2010, pp. 1–8, doi: 10.1109/OCEANSSYD.2010.5603591.

[32] A. Kim and R. M. Eustice, "Real-time visual SLAM for autonomous underwater hull inspection using visual saliency," *IEEE Trans. Robot.*, vol. 29, no. 3, pp. 719–733, Jun. 2013, doi: 10.1109/TRO.2012.2235699.

[33] E. Yang and D. Gu, "Nonlinear formation-keeping and mooring control of multiple autonomous underwater vehicles," *IEEE/ASME Trans. Mechatronics*, vol. 12, no. 2, pp. 164–178, Apr. 2007, doi: 10.1109/TMECH.2007.892826.

[34] S.-W. Huang, E. Chen, and J. Guo, "Efficient seafloor classification and submarine cable route design using an autonomous underwater vehicle," *IEEE J. Ocean. Eng.*, vol. 43, no. 1, pp. 7–18, Jan. 2018, doi: 10.1109/JOE.2017.2686558.

[35] T. Mercy, R. Van Parys, and G. Pipeleers, "Spline-based motion planning for autonomous guided vehicles in a dynamic environment," *IEEE Trans. Control. Syst. Technol.*, vol. 26, no. 6, pp. 2182–2189, Nov. 2018, doi: 10.1109/TCST.2017.2739706.

[36] A. Ye, H. Zhu, Z. Xu, C. Sun, and K. Yuan, "A vision-based guidance method for autonomous guided vehicles," in *Proc. IEEE Int. Conf. Mechatronics Automat.*, Aug. 2012, pp. 2025–2030, doi: 10.1109/ICMA.2012.6285133.

[37] G. Meyer, J. Dokic, and B. Müller, "Elements of a European roadmap on smart systems for automated driving," in *Road Vehicle Automation 2*. Cham, Switzerland: Springer, 2015, pp. 153–159.

[38] A. Taeihagh and H. S. M. Lim, "Governing autonomous vehicles: Emerging responses for safety, liability, privacy, cybersecurity, and industry risks," *Transp. Rev.*, vol. 39, no. 1, pp. 103–128, Jul. 2018.

[39] Q. Li, L. Chen, M. Li, S.-L. Shaw, and A. Nuchter, "A sensor-fusion drivable-region and lane-detection system for autonomous vehicle navigation in challenging road scenarios," *IEEE Trans. Veh. Technol.*, vol. 63, no. 2, pp. 540–555, Feb. 2014.

[40] J. Cohen. (May 22, 2018). *Sensor Fusion—Towards Data Science*. Accessed: Mar. 14, 2021. [Online]. Available: https://towardsdatascience.com/sensor-fusion-90135614fde6

[41] J. Z. Varghese and R. G. Boone, "Overview of autonomous vehicle sensors and systems," in *Proc. Int. Conf. Oper. Excellence Service Eng.*, 2015, pp. 178–191.

[42] R. Jirawimut, P. Ptasinski, V. Garaj, F. Cecelja, and W. Balachandran, "A method for dead reckoning parameter correction in pedestrian navigation system," *IEEE Trans. Instrum. Meas.*, vol. 52, no. 1, pp. 209–215, Feb. 2003.

[43] L. Tang, Y. Shi, Q. He, A. W. Sadek, and C. Qiao, "Performance test of autonomous vehicle LiDAR sensors under different weather conditions," *Transp. Res. Rec., J. Transp. Res. Board*, vol. 2674, no. 1, pp. 319–329, Jan. 2020.

[44] W. Xu, C. Yan, W. Jia, X. Ji, and J. Liu, "Analyzing and enhancing the security of ultrasonic sensors for autonomous vehicles," *IEEE Internet Things J.*, vol. 5, no. 6, pp. 5015–5029, Dec. 2018.

[45] Y. Zein, M. Darwiche, and O. Mokhiamar, "GPS tracking system for autonomous vehicles," *Alexandria Eng. J.*, vol. 57, no. 4, pp. 3127–3137, Dec. 2018.

[46] A. Zaarane, I. Slimani, W. Al Okaishi, I. Atouf, and A. Hamdoun, "Distance measurement system for autonomous vehicles using stereo camera," *Array*, vol. 5, Mar. 2020, Art. no. 100016.

[47] I. Bilik, O. Longman, S. Villeval, and J. Tabrikian, "The rise of radar for autonomous vehicles: Signal processing solutions and future research directions," *IEEE Signal Process. Mag.*, vol. 36, no. 5, pp. 20–31, Sep. 2019.

[48] SAE. *SAE Standards News: J3016 Automated-Driving Graphic Update*. Accessed: Feb. 8, 2021. [Online]. Available: https://www.sae.org/news/2019/01/sae-updates-j3016-automated-driving-graphic

[49] Analog. *Autonomous Transportation & ADAS*. Accessed: Jun. 4, 2021. [Online]. Available: https://www.analog.com/en/applications/markets/automotive-pavilion-home/autonomous-transportation-and-adas.html

[50] W. Maddern, A. Stewart, C. McManus, B. Upcroft, W. Churchill, and P. Newman, "Illumination invariant imaging: Applications in robust vision-based localisation, mapping and classification for autonomous vehicles," in *Proc. Vis. Place Recognit. Changing Environments Workshop, IEEE Int. Conf. Robot. Automat. (ICRA)*, vol. 2, May 2014, p. 3.

[51] Steve. (Jan. 23, 2020). *SAE Self-Driving Levels 0 to 5 for Automation—What They Mean—AutoPilot Review*. Accessed: Mar. 5, 2021. [Online]. Available: https://www.autopilotreview.com/self-driving-cars-sae-levels/

[52] *Naval History and Heritage Command*. Accessed: Jun. 10, 2021. [Online]. Available: https://www.history.navy.mil/research/library/online-reading-room/title-list-alphabetically/s/submarine-turtle-naval-documents.html

[53] D. R. Blidberg, "The development of autonomous underwater vehicles (AUVs); a brief summary," in *Proc. IEEE Int. Conf. Robot. Adaptation*, vol. 6500, 2010, pp. 1–12.

[54] D. S. Terracciano, L. Bazzarello, A. Caiti, R. Costanzi, and V. Manzari, "Marine robots for underwater surveillance," *Current Robot. Rep.*, vol. 1, no. 4, pp. 159–167, Dec. 2020, doi: 10.1007/s43154-020-00028-z.

[55] Woods Hole Oceanographic Institution. (Feb. 6, 2019). *Underwater Vehicles*. Accessed: May 13, 2021. [Online]. Available: https://www.whoi.edu/know-your-ocean/ocean-topics/tools-technology/underwater-vehicles/

[56] MBARI. (May 23, 2018). *Autonomous Underwater Vehicles*. [Online]. Available: https://www.mbari.org/at-sea/vehicles/autonomous-underwater-vehicles/

[57] A. Reyna, C. Martín, J. Chen, E. Soler, and M. Díaz, "On blockchain and its integration with IoT. Challenges and opportunities," *Future Gener. Comput. Syst.*, vol. 88, pp. 173–190, Nov. 2018, doi: 10.1016/j.future.2018.05.046.

[58] G. Rathee, A. Sharma, R. Iqbal, M. Aloqaily, N. Jaglan, and R. Kumar, "A blockchain framework for securing connected and autonomous vehicles," *Sensors*, vol. 19, no. 14, p. 3165, Jul. 2019, doi: 10.3390/s19143165.

[59] Z. Abubaker, M. U. Gurmani, T. Sultana, S. Rizwan, M. Azeem, M. Z. Iftikhar, and N. Javaid, "Decentralized mechanism for hiring the smart autonomous vehicles using blockchain," in *Proc. Int. Conf. Broadband Wireless Comput., Commun. Appl.*, in Lecture Notes in Networks and Systems, vol. 97, 2020, pp. 733–746.

[60] A. Islam and S. Y. Shin, "Blockchain-based UAV-assisted underwater monitoring on internet of underwater things," in *Proc. Symp. Korean Inst. Commun. Inf. Sci.*, Gangwon-do, South Korea, 2019, pp. 120–121.

[61] P. Abishek, S. M. Sundar, G. Shanmuga, B. Mathesh, T. Sairam, and P. Rajkumar, "Design, analysis, and development of autonomous underwater vehicle," *Int. J. Innov. Technol. Exploring Eng.*, vol. 9, no. 2, pp. 3805–3810, 2019, doi: 10.35940/ijitee.a5305.129219.

[62] T. Hyakudome, "Design of autonomous underwater vehicle," *Int. J. Adv. Robot. Syst.*, vol. 8, no. 1, pp. 131–139, 2011.

[63] T. Kim and J. Yuh, "Development of a real-time control architecture for a semi-autonomous underwater vehicle for intervention missions," *Control Eng. Pract.*, vol. 12, no. 12, pp. 1521–1530, 2004, doi: 10.1016/j.conengprac.2003.12.015.
[64] Defence Research and Development Organisation, Ministry of Defence, Government of India. *Naval Science & Technological Laboratory (NSTL)*. Accessed: May 16, 2021. [Online]. Available: https://www.drdo.gov.in/labs-and-establishments/naval-science-technological-laboratory-nstl
[65] S. K. Ravichandran and R. Rajavel, "Studies on autonomous underwater vehicle systems," *Int. J. Current Res.*, vol. 6, no. 7, pp. 7453–7457, Jul. 2014.
[66] R. Pérez-Alcocer, L. A. Torres-Méndez, E. Olguín-Díaz, and A. A. Maldonado-Ramírez, "Vision-based autonomous underwater vehicle navigation in poor visibility conditions using a model-free robust control," *J. Sensors*, vol. 2016, pp. 1–16, Jul. 2016, doi: 10.1155/2016/8594096.
[67] K. L. Vasudev, "Review of autonomous underwater vehicles," in *Autonomous Vehicles*. London, U.K.: IntechOpen, 2020. Accessed: May 15, 2021. [Online]. Available: https://www.intechopen.com/books/autonomous-vehicles/review-of-autonomous-underwater-vehicles
[68] I. Jawhar, N. Mohamed, J. Al-Jaroodi, and Z. Sheng, "An architecture for using autonomous underwater vehicles in wireless sensor networks for underwater pipeline monitoring," *IEEE Trans. Ind. Informat.*, vol. 15, no. 3, pp. 1329–1340, Mar. 2019, doi: 10.1109/TII.2018.2848290.
[69] V. Chalkiadakis, N. Papandroulakis, G. Livanos, K. Moirogiorgou, G. Giakos, and M. Zervakis, "Designing a small-sized autonomous underwater vehicle architecture for regular periodic fish-cage net inspection," in *Proc. IEEE Int. Conf. Imag. Syst. Techn. (IST)*, Oct. 2017, pp. 1–6, doi: 10.1109/IST.2017.8261525.
[70] L. Lapierre, "Robust diving control of an AUV," *Ocean Eng.*, vol. 36, no. 1, pp. 92–104, 2009, doi: 10.1016/j.oceaneng.2008.10.006.
[71] R. Eustice, H. Brown, and A. Kim, "An overview of AUV algorithms research and testbed at the university of Michigan," in *Proc. IEEE/OES Auton. Underwater Vehicles*, Oct. 2008, pp. 1–9, doi: 10.1109/AUV.2008.5290531.
[72] D. Goldberg, "Huxley: A flexible robot control architecture for autonomous underwater vehicles," in *Proc. IEEE OCEANS*, Jun. 2011, pp. 1–10, doi: 10.1109/Oceans-Spain.2011.6003512.
[73] Militaryaerospace. (Oct. 15, 2019). *Unmanned Underwater Vehicles UUV Artificial Intelligence*. Accessed: May 16, 2021. [Online]. Available: https://www.militaryaerospace.com/unmanned/article/14068665/unmanned-underwater-vehicles-uuv-artificial-intelligence
[74] L. L. Whitcomb, "Underwater robotics: Out of the research laboratory and into the field," in *Proc. Millennium Conf., IEEE Int. Conf. Robot. Automat. Symp. (ICRA)*, vol. 1, Apr. 2000, pp. 709–716, doi: 10.1109/robot.2000.844135.
[75] A. Gerardo, C. Hugo, C. Oscar, and R. Silvano, "AI-based path planner for an autonomous underwater vehicle," in *Proc. 6th WSEAS Int. Conf. Robot., Control Manuf. Technol.*, 2006, pp. 153–158.
[76] L. M. Aristizábal, S. Rúa, C. E. Gaviria, S. P. Osorio, C. A. Zuluaga, N. L. Posada, and R. E. Vásquez, "Design of an open source-based control platform for an underwater remotely operated vehicle," *Dyna*, vol. 83, no. 195, pp. 198–205, Feb. 2016, doi: 10.15446/dyna.v83n195.49828.
[77] D. Gračanin, K. P. Valavanis, and M. Matijašević, "Virtual environment testbed for autonomous underwater vehicles," *Control Eng. Pract.*, vol. 6, no. 5, pp. 653–660, 1998, doi: 10.1016/S0967-0661(98)00059-8.
[78] K. Alam, T. Ray, and S. G. Anavatti, "Design and construction of an autonomous underwater vehicle," *Neurocomputing*, vol. 142, pp. 16–29, Oct. 2014, doi: 10.1016/j.neucom.2013.12.055.
[79] N. Palomeras, J. C. García, M. Prats, J. J. Fernández, P. J. Sanz, and P. Ridao, "A distributed architecture for enabling autonomous underwater intervention missions," in *Proc. IEEE Int. Syst. Conf.*, Apr. 2010, pp. 159–164, doi: 10.1109/SYSTEMS.2010.5482349.
[80] A. Shumsky, "Fault diagnosis of sensors in the autonomous underwater vehicle: Adaptive quasi-linear parity relations method," *IFAC Proc. Volumes*, vol. 6, no. 1, pp. 384–389, 2006, doi: 10.3182/20060829-4-CN-2909.00063.
[81] G. Fenech. (Oct. 30, 2018). The link between autonomous vehicles and blockchain. Forbes. Accessed: May 16, 2021. [Online]. Available: https://www.forbes.com/sites/geraldfenech/2018/10/30/the-link-between-autonomous-vehicles-and-blockchain/?sh=686ef3f765a2
[82] M. A. Uddin, A. Stranieri, I. Gondal, and V. Balasurbramanian, "A lightweight blockchain based framework for underwater IoT," *Electronics*, vol. 8, no. 12, p. 1552, Dec. 2019, doi: 10.3390/electronics8121552.
[83] L. Yin, D. Chen, H. Gu, N. Guan, R. Zhang, and H. Hou, "Studies on situation reasoning approach of autonomous underwater vehicle under uncertain environment," *CAAI Trans. Intell. Technol.*, vol. 6, no. 2, pp. 235–250, Jun. 2021.
[84] D. Gomes, A. F. M. S. Saif, and D. Nandi, "Robust underwater object detection with autonomous underwater vehicle: A comprehensive study," in *Proc. Int. Conf. Comput. Adv.*, Jan. 2020, pp. 1–10.
[85] Y. Xu, T. Li, and S. Tong, "Event-triggered adaptive fuzzy bipartite consensus control of multiple autonomous underwater vehicles," *IET Control Theory Appl.*, vol. 14, no. 20, pp. 3632–3642, Dec. 2020.
[86] X. Liang, X. Qu, N. Wang, R. Zhang, and Y. Li, "Three-dimensional trajectory tracking of an underactuated AUV based on fuzzy dynamic surface control," *IET Intell. Transp. Syst.*, vol. 14, no. 5, pp. 364–370, 2020.
[87] L. Liu, L. Zhang, and S. Zhang, "Robust PIλ controller design for AUV motion control with guaranteed frequency and time domain behaviour," *IET Control Theory Appl.*, vol. 15, no. 5, pp. 784–792, Mar. 2021.
[88] K. Wrobel and A. Weintrit, "With regard to the autonomy in maritime operations—Hydrography and shipping, interlinked," *TransNav, Int. J. Mar. Navigat. Saf. Sea Transp.*, vol. 14, no. 3, pp. 745–749, 2020.
[89] C. Hu, Y. Pu, F. Yang, R. Zhao, A. Alrawais, and T. Xiang, "Secure and efficient data collection and storage of IoT in smart ocean," *IEEE Internet Things J.*, vol. 7, no. 10, pp. 9980–9994, Oct. 2020.
[90] F. Bonin-Font and A. B. Burguera, "NetHALOC: A learned global image descriptor for loop closing in underwater visual SLAM," *Expert Syst.*, vol. 38, no. 2, p. e12635, Mar. 2021.
[91] M. A. Hannan, S. Habib, M. S. Javadi, S. A. Samad, A. M. Muad, and A. Hussain, "Inter-vehicle wireless communications technologies, issues and challenges," *Inf. Technol. J.*, vol. 12, no. 4, pp. 558–568, Apr. 2013.
[92] K. C. Dey, A. Rayamajhi, M. Chowdhury, P. Bhavsar, and J. Martin, "Vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communication in a heterogeneous wireless network—Performance evaluation," *Transp. Res. C, Emerg. Technol.*, vol. 68, pp. 168–184, Jul. 2016.
[93] S. Campbell, N. O'Mahony, L. Krpalcova, D. Riordan, J. Walsh, A. Murphy, and C. Ryan, "Sensor technology in autonomous vehicles: A review," in *Proc. 29th Irish Signals Syst. Conf. (ISSC)*, 2018, pp. 1–4.
[94] A. Farooq, Q. Z. Ahmed, and T. Alade, "Indoor two way ranging using mm-Wave for future wireless networks," Univ. Huddersfield, U.K., Tech. Rep., 2019.
[95] Z. Wang, Y. Wu, and Q. Niu, "Multi-sensor fusion in automated driving: A survey," *IEEE Access*, vol. 8, pp. 2847–2868, 2020.
[96] G. Toulminet, M. Bertozzi, S. Mousset, A. Bensrhair, and A. Broggi, "Vehicle detection by means of stereo vision-based obstacles features extraction and monocular pattern analysis," *IEEE Trans. Image Process.*, vol. 15, no. 8, pp. 2364–2375, Aug. 2006.
[97] R. Adamshuk, D. Carvalho, J. H. Z. Neme, E. Margraf, S. Okida, A. Tusset, M. M. Santos, R. Amaral, A. Ventura, and S. Carvalho, "On the applicability of inverse perspective mapping for the forward distance estimation based on the HSV colormap," in *Proc. IEEE Int. Conf. Ind. Technol. (ICIT)*, Mar. 2017, pp. 1036–1041.
[98] J. Han, O. Heo, M. Park, S. Kee, and M. Sunwoo, "Vehicle distance estimation using a mono-camera for FCW/AEB systems," *Int. J. Automot. Technol.*, vol. 17, no. 3, pp. 483–491, Jun. 2016.
[99] M. Rezaei, M. Terauchi, and R. Klette, "Robust vehicle detection and distance estimation under challenging lighting conditions," *IEEE Trans. Intell. Transp. Syst.*, vol. 16, no. 5, pp. 2723–2743, Oct. 2015.
[100] D. Zhao, Y. Yang, J. Huang, and Y. Liu, "Vehicle position estimation using geometric constants in traffic scene," in *Proc. IEEE Int. Conf. Service Oper. Logistics, Informat.*, Oct. 2014, pp. 90–95.
[101] F. Oniga, S. Nedevschi, and M. M. Meinecke, "Curb detection based on a multi-frame persistence map for urban driving scenarios," in *Proc. 11th Int. IEEE Conf. Intell. Transp. Syst.*, Oct. 2008, pp. 67–72.
[102] J. Siegemund, "Curb reconstruction using conditional random fields," in *Proc. IEEE Intell. Vehicles Symp*, Jun. 2010, pp. 203–210.
[103] L. Wang, T. Wu, Z. Xiao, L. Xiao, D. Zhao, and J. Han, "Multi-cue road boundary detection using stereo vision," in *Proc. IEEE Int. Conf. Veh. Electron. Saf. (ICVES)*, Jul. 2016, pp. 1–6.
[104] Y. Kang, C. Roh, S.-B. Suh, and B. Song, "A LiDAR-based decision-making method for road boundary detection using multiple Kalman filters," *IEEE Trans. Ind. Electron.*, vol. 59, no. 11, pp. 4360–4368, Nov. 2012.

[105] S. Peng, "A robust detection algorithm for urban road boundaries based on 3D LiDAR," *J. Zhejiang Univ.*, vol. 52, no. 3, pp. 504–514, 2018.
[106] K. Hu, "Real-time extraction method of road boundary based on three-dimensional LiDAR," *J. Phys., Conf. Ser.*, vol. 1074, no. 1, p. 258, 2018.
[107] H. Wang, H. Luo, C. Wen, J. Cheng, P. Li, Y. Chen, C. Wang, and J. Li, "Road boundaries detection based on local normal saliency from mobile laser scanning data," *IEEE Geosci. Remote Sens. Lett.*, vol. 12, no. 10, pp. 2085–2089, Oct. 2015.
[108] D. Zai, J. Li, Y. Guo, M. Cheng, Y. Lin, H. Luo, and C. Wang, "3-D road boundary extraction from mobile laser scanning data via supervoxels and graph cuts," *IEEE Trans. Intell. Transp. Syst.*, vol. 19, no. 3, pp. 802–813, Mar. 2018.
[109] W. Yao, Z. Deng, and L. Zhou, "Road curb detection using 3D LiDAR and integral laser points for intelligent vehicles," in *Proc. 6th Int. Conf. Soft Comput. Intell. Syst.*, Nov. 2012, pp. 100–105.
[110] G. Wang, J. Wu, R. He, and S. Yang, "A point cloud-based robust road curb detection and tracking method," *IEEE Access*, vol. 7, pp. 24611–24625, 2019.
[111] X. Lu, Y. Ai, and B. Tian, "Real-time mine road boundary detection and tracking for autonomous truck," *Sensors*, vol. 20, no. 4, p. 1121, Feb. 2020.
[112] S. Kuutti, S. Fallah, K. Katsaros, M. Dianati, F. Mccullough, and A. Mouzakitis, "A survey of the state-of-the-art localization techniques and their potentials for autonomous vehicle applications," *IEEE Internet Things J.*, vol. 5, no. 2, pp. 829–846, Apr. 2018.
[113] X. Cheng, R. Zhang, and L. Yang, "Wireless toward the era of intelligent vehicles," *IEEE Internet Things J.*, vol. 6, no. 1, pp. 188–202, Feb. 2019.
[114] B. Hu, L. Fang, X. Cheng, and L. Yang, "In-vehicle caching (IV-cache) via dynamic distributed storage relay (D^2SR) in vehicular networks," *IEEE Trans. Veh. Technol.*, vol. 68, no. 1, pp. 843–855, Nov. 2019.
[115] Z. Li, W. Trappe, Y. Zhang, and B. Nath, "Robust statistical methods for securing wireless localization in sensor networks," in *Proc. 4th Int. Symp. Inf. Process. Sensor Netw. (IPSN)*, 2005, pp. 91–98.
[116] D. Wang, J. Wan, M. Wang, and Q. Zhang, "An MEF-based localization algorithm against outliers in wireless sensor networks," *Sensors*, vol. 16, no. 7, p. 1041, Jul. 2016.
[117] M. B. Shanthi and D. K. Anvekar, "Secure localization for underwater wireless sensor networks based on probabilistic approach," in *Proc. 2nd Int. Conf. Adv. Electron., Comput. Commun. (ICAECC)*, Feb. 2018, pp. 1–6.
[118] D. Liu, P. Ning, A. Liu, C. Wang, and W. K. Du, "Attack-resistant location estimation in wireless sensor networks," *ACM Trans. Inf. Syst. Secur.*, vol. 11, no. 4, pp. 1–39, Jul. 2008.
[119] C. Wang, A. Liu, and P. Ning, "Cluster-based minimum mean square estimation for secure and resilient localization in wireless sensor networks," in *Proc. Int. Conf. Wireless Algorithms, Syst. Appl. (WASA)*, Aug. 2007, pp. 29–37.
[120] S. A. AlRoomi, I. Ahmad, and T. Dimitriou, "Secure localization using hypothesis testing in wireless networks," *Ad Hoc Netw.*, vol. 74, pp. 47–56, May 2018.
[121] X. Liu, S. Su, F. Han, Y. Liu, and Z. Pan, "A range-based secure localization algorithm for wireless sensor networks," *IEEE Sensors J.*, vol. 19, no. 2, pp. 785–796, Jan. 2019.
[122] W. Pi, P. Yang, D. Duan, C. Chen, X. Cheng, L. Yang, and H. Li, "Malicious user detection for cooperative mobility tracking in autonomous driving," *IEEE Internet Things J.*, vol. 7, no. 6, pp. 4922–4936, Jun. 2020.
[123] *Data is the New Oil in the Future of Automated Driving*, Intel.com, Nov. 2016. Accessed: Sep. 18, 2021. [Online]. Available: https://newsroom.intel.com/editorials/krzanich-the-future-of-automated-driving/
[124] C. Kaiser, M. Steger, A. Dorri, A. Festl, A. Stocker, M. Fellmann, and S. Kanhere, "Towards a privacy-preserving way of vehicle data sharing—A case for blockchain technology?" in *Advanced Microsystems for Automotive Applications*. Cham, Switzerland: Springer, 2019, pp. 111–122.
[125] Home. *Automat-Project.eu*. Accessed: Sep. 18, 2021. [Online]. Available: https://automat-project.eu/
[126] C. S. Wright, "Bitcoin: A peer-to-peer electronic cash system," *SSRN Electron. J.*, pp. 1–12, Aug. 2019.
[127] L. Zhang, "Key management scheme for secure channel establishment in fog computing," *IEEE Trans. Cloud Comput.*, vol. 9, no. 3, pp. 1117–1128, Jul. 2021.
[128] M. S. Ali, M. Vecchio, M. Pincheira, K. Dolui, F. Antonelli, and M. H. Rehmani, "Applications of blockchains in the Internet of Things: A comprehensive survey," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 2, pp. 1676–1717, 2nd Quart., 2019.
[129] S. Rowan, M. Clear, M. Gerla, M. Huggard, and C. Mc Goldrick, "Securing vehicle to vehicle communications using blockchain through visible light and acoustic side-channels," 2017, *arXiv:1704.02553*. [Online]. Available: http://arxiv.org/abs/1704.02553
[130] R. Barber, "Autonomous vehicle communication using blockchain," Sally McDonnell Barksdale Honors College, Univ. Mississippi, Oxford, MS, USA, Tech. Rep. 789, 2018.
[131] S. Mitra, S. Bose, S. S. Gupta, and A. Chattopadhyay, "Secure and tamper-resilient distributed ledger for data aggregation in autonomous vehicles," in *Proc. IEEE Asia Pacific Conf. Circuits Syst. (APCCAS)*, Oct. 2018, pp. 548–551.
[132] M. Singh and S. Kim, "Trust bit: Reward-based intelligent vehicle commination using blockchain paper," in *Proc. IEEE 4th World Forum Internet Things (WF-IoT)*, Feb. 2018, pp. 62–67.
[133] C. Oham, R. Jurdak, S. S. Kanhere, A. Dorri, and S. Jha, "B-FICA: BlockChain based framework for auto-insurance claim and adjudication," 2018, *arXiv:1806.06169*. [Online]. Available: http://arxiv.org/abs/1806.06169
[134] Arora and S. K. Yadav, "Blockchain-based security mechanism for the internet of vehicles (IoV)," *SSRN Electron. J.*, pp. 1–6, Apr. 2018, doi: 10.2139/ssrn.3166721.
[135] H. Liu, Y. Zhang, and T. Yang, "Blockchain-enabled security in electric vehicles cloud and edge computing," *IEEE Netw.*, vol. 32, no. 3, pp. 78–83, May/Jun. 2018.
[136] Z. Su, Y. Wang, Q. Xu, M. Fei, Y.-C. Tian, and N. Zhang, "A secure charging scheme for electric vehicles with smart communities in energy blockchain," *IEEE Internet Things J.*, vol. 6, no. 3, pp. 4601–4613, Jun. 2019.
[137] S. Hua, E. Zhou, B. Pi, J. Sun, Y. Nomura, and H. Kurihara, "Apply blockchain technology to electric vehicle battery refueling," in *Proc. 51st Hawaii Int. Conf. Syst. Sci.*, 2018, pp. 1–8.
[138] M. Singh and S. Kim, "Blockchain based intelligent vehicle data sharing framework," 2017, *arXiv:1708.09721*. [Online]. Available: https://arxiv.org/abs/1708.09721
[139] A. Buzachis, A. Celesti, A. Galletta, M. Fazio, and M. Villari, "A secure and dependable multi-agent autonomous intersection management (MA-AIM) system leveraging blockchain facilities," in *Proc. IEEE/ACM Int. Conf. Utility Cloud Comput. Companion (UCC Companion)*, Dec. 2018, pp. 226–231.
[140] H. Guo, E. Meamari, and C.-C. Shen, "Blockchain-inspired event recording system for autonomous vehicles," 2018, *arXiv:1809.04732*. [Online]. Available: http://arxiv.org/abs/1809.04732
[141] C. Oham, S. S. Kanhere, R. Jurdak, and S. Jha, "A blockchain-based liability attribution framework for autonomous vehicles," 2018, *arXiv:abc/1802.05050*. [Online]. Available: https://arxiv.org/abs/1802.05050
[142] H. Guo, W. Li, M. Nejad, and C.-C. Shen, "Proof-of-event recording system for autonomous vehicles: A blockchain-based solution," *IEEE Access*, vol. 8, pp. 182776–182786, 2020.
[143] G. Rathee, A. Sharma, R. Iqbal, M. Aloqaily, N. Jaglan, and R. Kumar, "A blockchain framework for securing connected and autonomous vehicles," *Sensors*, vol. 19, no. 14, p. 3165, Jul. 2019.
[144] M. Baza, M. Nabil, N. Lasla, K. Fidan, M. Mahmoud, and M. Abdallah, "Blockchain-based firmware update scheme tailored for autonomous vehicles," 2018, *arXiv:1811.05905*. [Online]. Available: http://arxiv.org/abs/1811.05905
[145] X. Huang, Y. Zhang, D. Li, and L. Han, "An optimal scheduling algorithm for hybrid EV charging scenario using consortium blockchains," *Future Gener. Comput. Syst.*, vol. 91, pp. 555–562, Feb. 2018.
[146] J. Kang, R. Yu, X. Huang, S. Maharjan, Y. Zhang, and E. Hossain, "Enabling localized peer-to-peer electricity trading among plug-in hybrid electric vehicles using consortium blockchains," *IEEE Trans. Ind. Informat.*, vol. 13, no. 6, pp. 3154–3164, Dec. 2017.
[147] W. Li, H. Guo, M. Nejad, and C.-C. Shen, "Privacy-preserving traffic management: A blockchain and zero-knowledge proof inspired approach," *IEEE Access*, vol. 8, pp. 181733–181743, 2020.
[148] S. Wang, Y. Yuan, X. Wang, J. Li, R. Qin, and F.-Y. Wang, "An overview of smart contract: Architecture, applications, and future trends," in *Proc. IEEE Intell. Vehicles Symp. (IV)*, Jun. 2018, pp. 108–113.
[149] A. Wright and P. De Filippi, "Decentralized blockchain technology and the rise of Lex cryptographia," *SSRN Electron. J.*, pp. 1–58, Mar. 2015. [Online]. Available: https://ssrn.com/abstract=2580664
[150] M. Alharby, A. Aldweesh, and A. V. Moorsel, "Blockchain-based smart contracts: A systematic mapping study of academic research (2018)," in *Proc. Int. Conf. Cloud Comput., Big Data Blockchain (ICCBB)*, Nov. 2018, pp. 1–6.

[151] D. Macrinici, C. Cartofeanu, and S. Gao, "Smart contract applications within blockchain technology: A systematic mapping study," *Telematics Inform.*, vol. 35, no. 8, pp. 2337–2354, 2018.
[152] N. Zhao and H. Wu, "Blockchain combined with smart contract to keep safety energy trading for autonomous vehicles," in *Proc. IEEE 89th Veh. Technol. Conf. (VTC-Spring)*, Apr. 2019, pp. 1–5.
[153] J. Wang, L. Zhang, Y. Huang, and J. Zhao, "Safety of autonomous vehicles," *J. Adv. Transp.*, vol. 2020, pp. 1–13, Oct. 2020.
[154] J. M. Anderson, N. Kalra, K. D. Stanley, P. Sorensen, C. Samaras, and O. A. Oluwatola, *Autonomous Vehicle Technology: A Guide for Policymakers*. Santa Monica, CA, USA: RAND Corporation, 2016.
[155] F. M. Favarò, N. Nader, S. O. Eurich, M. Tripp, and N. Varadaraju, "Examining accident reports involving autonomous vehicles in California," *PLoS ONE*, vol. 12, no. 9, Sep. 2017, Art. no. e0184952.
[156] T. Raviteja and I. S. R. Vedaraj, "An introduction of autonomous vehicles and a brief survey," *J. Crit. Rev.*, vol. 7, no. 13, pp. 196–202, 2020.
[157] R. E. Stern, Y. Chen, M. Churchill, F. Wu, M. L. D. Monache, B. Piccoli, B. Seibold, J. Sprinkle, and D. B. Work, "Quantifying air quality benefits resulting from few autonomous vehicles stabilizing traffic," *Transp. Res. D, Transp. Environ.*, vol. 67, pp. 351–365, Feb. 2019.
[158] *Critical Reasons for Crashes Investigated in the National Motor Vehicle Crash Causation Survey*, U.S. Dept. Transp. Nat. Highway Traffic Saf. Admin., Washington, DC, USA, 2015.
[159] A. Faisal, T. Yigitcanlar, M. Kamruzzaman, and G. Currie, "Understanding autonomous vehicles: A systematic literature review on capability, impact, planning and policy," *J. Transp. Land Use*, vol. 12, no. 1, pp. 45–72, Jan. 2019.
[160] T. Litman, "Autonomous vehicle implementation predictions implications for transport planning report," Victoria Transp. Policy Inst., Nat. Acad. Sci., Eng., Med., Tech. Rep., Mar. 2021, pp. 1–39.
[161] D. Gerrard, "Greater energy efficiency via self-driving cars," Stanford Univ., Stanford, CA, USA, Tech. Rep., Dec. 2014. Accessed: Sep. 19, 2021. [Online]. Available: http://large.stanford.edu/courses/2014/ph240/gerrard2/
[162] A. Vahidi and A. Sciarretta, "Energy saving potentials of connected and automated vehicles," *Transp. Res. C, Emerg. Technol.*, vol. 95, pp. 822–843, Oct. 2018.
[163] A. O. Al-Jazaeri, L. Samaranayake, S. Longo, and D. J. Auger, "Fuzzy logic control for energy saving in autonomous electric vehicles," in *Proc. IEEE Int. Electr. Vehicle Conf. (IEVC)*, Florence, Italy, Dec. 2014, pp. 17–19.
[164] A. Manimuthu, V. Dharshini, I. Zografopoulos, M. K. Priyan, and C. Konstantinou, "Contactless technologies for smart cities: Big data, IoT, and cloud infrastructures," *Social Netw. Comput. Sci.*, vol. 2, no. 4, pp. 1–24, Jul. 2021.
[165] L. Tate, "Energy efficiency of autonomous car powertrain," SAE Tech. Paper 2018-01-1092, Aug. 2018.
[166] I. Holovatenko and A. Pysarenko, "Energy-efficient path-following control system of automated guided vehicles," *J. Control, Autom. Electr. Syst.*, vol. 32, pp. 667–679, Jan. 2021.
[167] I. Zografopoulos, J. Ospina, X. Liu, and C. Konstantinou, "Cyber-physical energy systems security: Threat modeling, risk assessment, resources, metrics, and case studies," *IEEE Access*, vol. 9, pp. 29775–29818, 2021, doi: 10.1109/ACCESS.2021.3058403.
[168] K. Kaur, S. Garg, G. Kaddoum, N. Kumar, and F. Gagnon, "SDN-based internet of autonomous vehicles: An energy-efficient approach for controller placement," *IEEE Wireless Commun.*, vol. 26, no. 6, pp. 72–79, Dec. 2019.
[169] D. Zhao, "Towards energy efficient autonomous vehicles via cloud-aided learning," Dept. Aeronaut. Automot. Eng., Loughborough Univ., Loughborough, U.K., Tech. Rep., 2020. [Online]. Available: https://gtr.ukri.org/projects?ref=EP%2FS001956%2F1
[170] Home. *Automat-Project.eu*. Accessed: Sep. 18, 2021. [Online]. Available: https://automat-project.eu/
[171] *Automated, Connected, and Electric Vehicle Systems*, Steven Underwood, Expert Forecast Roadmap Sustain. Transp., Inst. Adv. Vehicle Syst. Univ. Michigan, Dearborn, MI, USA, Tech. Rep., Dec. 2014. Acccessed: Sep. 19, 2021. [Online]. Available: http://graham.umich.edu/media/files/LC-IA-Final-Underwood.pdf
[172] S. Zoria, "Smart cities: A new look at the autonomous-vehicle infrastructure," Startup, Nov. 2019. Accessed: Sep. 18, 2021. [Online]. Available: https://medium.com/swlh/smart-cities-a-new-look-at-the-autonomous-vehicle-infrastructure-3e00cf3e93b2
[173] D. Gritzalis, M. Theocharidou, and G. Stergiopoulos, "Critical infrastructure security and resilience," in *Advanced Sciences and Technologies for Security Applications*. USA: Springer, 2019.
[174] C. Konstantinou, M. Maniatakos, F. Saqib, S. Hu, J. Plusquellic, and Y. Jin, "Cyber-physical systems: A security perspective," in *Proc. 20th IEEE Eur. Test Symp. (ETS)*, May 2015, pp. 1–8, doi: 10.1109/ETS.2015.7138763.
[175] A. A. Alkheir, M. Aloqaily, and H. T. Mouftah, "Connected and autonomous electric vehicles (CAEVs)," *IT Prof.*, vol. 20, no. 6, pp. 54–61, Nov./Dec. 2018, doi: 10.1109/MITP.2018.2876977.
[176] I. W. Damaj, D. K. Serhal, L. A. Hamandi, R. N. Zantout, and H. T. Mouftah, "Connected and autonomous electric vehicles: Quality of experience survey and taxonomy," *Veh. Commun.*, vol. 28, Apr. 2021, Art. no. 100312.
[177] Z. Huang, Z. Li, C. S. Lai, Z. Zhao, X. Wu, X. Li, N. Tong, and L. L. Lai, "A novel power market mechanism based on blockchain for electric vehicle charging stations," *Electronics*, vol. 10, no. 3, p. 307, Jan. 2021.
[178] A. Hasankhani, S. M. Hakimi, M. Bisheh-Niasar, M. Shafie-Khah, and H. Asadolahi, "Blockchain technology in the future smart grids: A comprehensive review and frameworks," *Int. J. Electr. Power Energy Syst.*, vol. 129, Jul. 2021, Art. no. 106811.
[179] G. Subramanian and A. S. Thampy, "Implementation of hybrid blockchain in a pre-owned electric vehicle supply chain," *IEEE Access*, vol. 9, pp. 82435–82454, 2021.
[180] S. N. Gowda, B. A. Eraqi, H. Nazaripouya, and R. Gadh, "Assessment and tracking electric vehicle battery degradation cost using blockchain," in *Proc. IEEE Power Energy Soc. Innov. Smart Grid Technol. Conf. (ISGT)*, Feb. 2021, pp. 1–5.
[181] F. Jamil, O. Cheikhrouhou, H. Jamil, A. Koubaa, A. Derhab, and M. A. Ferrag, "PetroBlock: A blockchain-based payment mechanism for fueling smart vehicles," *Appl. Sci.*, vol. 11, no. 7, p. 3055, Mar. 2021.
[182] M. K. Thukral, "Blockchain-based smart contract design for crowdfunding electrical vehicle charging station setup," in *Electric Vehicles*. Singapore: Springer, 2021, pp. 187–198.
[183] Z. Wan, T. Zhang, W. Liu, M. Wang, and L. Zhu, "Decentralized privacy-preserving fair exchange scheme for V2G based on blockchain," *IEEE Trans. Dependable Secure Comput.*, early access, Feb. 15, 2021, doi: 10.1109/TDSC.2021.3059345.
[184] S. Distefano, A. D. Giacomo, and M. Mazzara, "Trustworthiness for transportation ecosystems: The blockchain vehicle information system," *IEEE Trans. Intell. Transp. Syst.*, vol. 22, no. 4, pp. 2013–2022, Apr. 2021.
[185] P. W. Shaikh and H. T. Mouftah, "Intelligent charging infrastructure design for connected and autonomous electric vehicles in smart cities," in *Proc. IFIP/IEEE IM Workshop, 4th Int. Workshop Intell. Transp. Auton. Vehicles Technol. (ITAVT)*, Bordeaux, France, May 2021, pp. 992–997.
[186] M. Campbell, M. Egerstedt, J. P. How, and R. M. Murray, "Autonomous driving in urban environments: Approaches, lessons and challenges," *Phil. Trans. Roy. Soc. A, Math., Phys. Eng. Sci.*, vol. 368, no. 1928, pp. 4649–4672, Oct. 2010.
[187] M. Azad, N. Hoseinzadeh, C. Brakewood, C. R. Cherry, and L. D. Han, "Fully autonomous buses: A literature review and future research directions," *J. Adv. Transp.*, vol. 2019, pp. 1–16, Dec. 2019.
[188] S. A. Bagloee, M. Tavana, M. Asadi, and T. Oliver, "Autonomous vehicles: Challenges, opportunities, and future implications for transportation policies," *J. Mod. Transp.*, vol. 24, no. 4, pp. 284–303, Dec. 2016.
[189] K. Bhadane, P. Sanjeevikumar, B. Khan, M. Thakre, A. Ahmad, T. Jaware, D. P. Patil, and A. S. Pande, "A comprising study on modernization of electric vehicle subsystems, challenges, opportunities and strategies for its further development," in *Proc. IEEE Conf. ICNTE*, New Mumbai, India, Jan. 2021, pp. 1–9.
[190] F. Un-Noor, S. Padmanaban, L. Mihet-Popa, M. N. Mollah, and E. Hossain, "A comprehensive study of key electric vehicle (EV) components, technologies, challenges, impacts, and future direction of development," *Energies*, vol. 10, pp. 1–82, Aug. 2017.
[191] H. Jahangir and C. Konstantinou, "Plug-in electric vehicles demand modeling in smart grids: A deep learning-based approach: Wip abstract," in *Proc. ACM/IEEE 12th Int. Conf. Cyber-Phys. Syst.*, May 2021, pp. 221–222.
[192] I. J. Martínez, J. Garcìa-Villalobos, I. Zamora, and P. Eguía, "Energy management of micro renewable energy source and electric vehicles at home level," *J. Mod. Power Syst. Clean Energy*, vol. 5, no. 6, pp. 979–990, Nov. 2017.
[193] M. Longo, "Electric vehicles integrated with renewable energy sources for sustainable mobility," in *New Trends in Electrical Vehicle Powertrains*. London, U.K.: Intechopen, 2018, pp. 203–223.
[194] Y. Ramsingar, "Overview of technical standard of electric vehicle/grid code used in electric vehicle," *Int. J. Mod. Trends Sci. Technol.*, vol. 6, no. 4, pp. 315–323, Apr. 2020.

[195] K. V. Bhadane, T. H. Jaware, D. P. Patil, and A. Nayyar, "Wind energy system grid integration and grid code requirements of wind energy system," in *Control and Operation of Grid-Connected Wind Energy Systems*. Cham, Switzerland: Springer, 2021, pp. 247–273.

[196] M. A. Hannan, M. M. Hoque, A. Mohamed, and A. Ayob, "Review of energy storage systems for electric vehicle applications: Issues and challenges," *Renew. Sustain. Energy Rev.*, vol. 69, pp. 771–789, Mar. 2017.

[197] C. Xenofontos, I. Zografopoulos, C. Konstantinou, A. Jolfaei, M. K. Khan, and K.-K. R. Choo, "Consumer, commercial and industrial IoT (In)security: Attack taxonomy and case studies," *IEEE Internet Things J.*, early access, May 13, 2021, doi: 10.1109/JIOT.2021.3079916.

[198] A. N. Vijay, "Overview of energy storage devices use in electric vehicles," *Int. J. Mod. Trends Sci. Technol.*, vol. 6, no. 4, pp. 303–307, Apr. 2020.

[199] A. Jain. (Jul. 2018). NPTEL electric vehicle part I. Department Electrical, IIT Delhi. [Online]. Available: https://nptel.ac.in/courses/108102121/

[200] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," *Decentralized Bus. Rev.*, vol. 21260, 2008.

[201] R. Cupek, M. Drewniak, M. Fojcik, E. Kyrkjebø, J. C.-W. Lin, D. Mrozek, K. Øvsthus, and A. Ziebinski, "Autonomous guided vehicles for smart industries—The state-of-the-art and research challenges," in *Proc. Int. Conf. Comput. Sci.*, 2020, pp. 330–343.

[202] O. Catal, S. Leroux, C. De Boom, T. Verbelen, and B. Dhoedt, "Anomaly detection for autonomous guided vehicles using Bayesian surprise," in *Proc. IEEE/RSJ Int. Conf. Intell. Robots Syst. (IROS)*, Oct. 2020, pp. 8148–8153, doi: 10.1109/IROS45743.2020.9341386.

[203] P. M. de Sant Ana, N. Marchenko, P. Popovski, and B. Soret, "Wireless control of autonomous guided vehicle using reinforcement learning," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2020, pp. 1–7, doi: 10.1109/GLOBECOM42002.2020.9322156.

[204] A. Sánchez-Sotano, A. Cerezo-Narváez, F. Abad-Fraga, A. Pastor-Fernández, and J. Salguero-Gómez, "Trends of digital transformation in the shipbuilding sector," in *New Trends in the Use of Artificial Intelligence for the Industry 4.0*. London, U.K.: IntechOpen, 2020, p. 3.

[205] J. Stillig and N. Parspour, "Novel autonomous guided vehicle system for the use in logistics applications," in *Advances in Automotive Production Technology—Theory and Application*. Berlin, Germany: Springer, 2021, pp. 424–432.

[206] W. Wang, Y. Wu, Z. Jiang, and J. Qi, "A clutter-resistant SLAM algorithm for autonomous guided vehicles in dynamic industrial environment," *IEEE Access*, vol. 8, pp. 109770–109782, 2020, doi: 10.1109/ACCESS.2020.3001756.

[207] *Warehouse Labor Planning—A Spreadsheet Template - logiwa blog*, Logiwa.com, Aug. 2021. Accessed: Sep. 18, 2021. [Online]. Available: https://www.logiwa.com/blog/warehouse-labor-planning

[208] *Case Study, How Much Does Automate Guided Vehicle (AGV) Maintenance Cost?* Accessed: Jun. 6, 2021. [Online]. Available: https://www.agvnetwork.com/case-study-automated-guided-vehicle-maintenance-cost

[209] *Bcg.com*. Accessed: Sep. 18, 2021. [Online]. Available: https://image-src.bcg.com/Images/BCG-Stamping-Out-Counterfeit-Goods-with-Blockchain-and-IoT-May-2019_tcm9-220027.pdf

[210] I. J. Jensen, D. F. Selvaraj, and P. Ranganathan, "Blockchain technology for networked swarms of unmanned aerial vehicles (UAVs)," in *Proc. IEEE 20th Int. Symp. World Wireless, Mobile Multimedia Netw. (WoWMoM)*, Jun. 2019, pp. 1–7.

[211] X. Li, Y. Wang, P. Vijayakumar, D. He, N. Kumar, and J. Ma, "Blockchain-based mutual-healing group key distribution scheme in unmanned aerial vehicles ad-hoc network," *IEEE Trans. Veh. Technol.*, vol. 68, no. 11, pp. 11309–11322, Sep. 2019.

[212] V. Sharma, F. Song, I. You, and M. Atiquzzaman, "Energy efficient device discovery for reliable communication in 5G-based IoT and BSNs using unmanned aerial vehicles," *J. Netw. Comput. Appl.*, vol. 97, pp. 79–95, Nov. 2017.

[213] E. C. Ferrer, "The blockchain: A new framework for robotic swarm systems," 2016, *arXiv:1608.00695*. [Online]. Available: http://arxiv.org/abs/1608.00695

[214] T. Hewa, M. Ylianttila, and M. Liyanage, "Survey on blockchain based smart contracts: Applications, opportunities and challenges," *J. Netw. Comput. Appl.*, vol. 177, Mar. 2021, Art. no. 102857.

[215] B. K. Mohanta, S. S. Panda, and D. Jena, "An overview of smart contract and use cases in blockchain technology," in *Proc. 9th Int. Conf. Comput., Commun. Netw. Technol. (ICCCNT)*, Jul. 2018, pp. 1–4.

[216] T. M. Fernández-Caramés, O. Blanco-Novoa, I. Froiz-Míguez, and P. Fraga-Lamas, "Towards an autonomous industry 4.0 warehouse: A UAV and blockchain-based system for inventory and traceability applications in big data-driven supply chain management," *Sensors*, vol. 19, no. 10, p. 2394, May 2019.

[217] *Facts + Statistics: Aviation and Drones*. Accessed: Jul. 16, 2021. [Online]. Available: https://www.iii.org/fact-statistic/facts-statistics-aviation-and-drones

[218] W. Zafar and B. M. Khan, "Flying ad-hoc networks: Technological and social implications," *IEEE Technol. Soc. Mag.*, vol. 35, no. 2, pp. 67–74, Jun. 2016.

[219] U. E. Franke, "Civilian drones: Fixing an image problem?" Ethz.ch. Accessed: Sep. 18, 2021. [Online]. Available: https://isnblog.ethz.ch/security/civilian-drones-fixing-an-image-problem

[220] A. C. Watts, V. G. Ambrosia, and E. A. Hinkley, "Unmanned aircraft systems in remote sensing and scientific research: Classification and considerations of use," *Remote Sens.*, vol. 4, no. 6, pp. 1671–1692, 2012.

[221] Jojo. (Feb. 3, 2017). *Types of Drones—Explore the Different Types of UAVs*. Accessed: Jul. 15, 2021. [Online]. Available: https://www.circuitstoday.com/types-of-drones

[222] A. Arjomandi, S. Agostino, M. Mammone, M. Nelson, and T. Zhou, "Classification of unmanned aerial vehicle," Mech. Eng., Univ. Adelaide, Adelaide, SA, Australia, Tech. Rep., 2006. Accessed: Sep. 19, 2021. [Online]. Available: https://d1wqtxts1xzle7.cloudfront.net/29666442/group9-with-cover-page-v2.pdf?Expires=1632057933&Signature=PNb85G9wBxd7As8nY7i9K5R5UcXjxZ4-gKJmRZ0p52R53ThTcNWP9yHPPulyc5l09mI-X2GnOsTOAPgMT6JF3aybDVsJ2brZAedsGYRIsChTudaTURF8mKao5pskRRjLVnBIeHUDdd5B81MyRGExuorUjhS0guqTz~RIKeMizoxFWj2-W3QPFKJ9YJluht6NSonAEVtMDY4Y0tdRbouWdskHoKBQp6KnwAwXqbtuXa2MObQ3Ewdbs41sTtWECQfRF3phC01wyEX0bexS8PW85TU0C1PtidpSwaIPtD13AIPXRIqHEnLUS9KGiyF6pwIQLvO3UZjNbws1c1fOWFTTLQ__&Key-Pair-Id=APKAJLOHF5GGSLRBV4ZA

[223] S. G. Gupta, M. Ghonge, and P. M. Jawandhiya, "Review of unmanned aircraft system (UAS)," *SSRN Electron. J.*, vol. 2, no. 4, pp. 1646–1658, Apr. 2013.

[224] A. Cavoukian, *Privacy and Drones: Unmanned Aerial Vehicles*. Toronto, ON, Canada: Information and Privacy Commissioner of Ontario, 2012.

[225] B. Zakora and A. Molodchick. *Classification of UAV*. Accessed: Jun. 11, 2021. [Online]. Available: http://read.meil.pw.pl/abstracts/StudentAbstract_Zakora Molodchik.pdf

[226] V. A. N. J. A. Stefanovic, M. I. L. I. C. A. Marjanovic, and M. I. L. A. N. Bajovic, "Conceptual system designs civil UAV for typical aerial work applications," in *Proc. 5th Int. Sci. Conf. Defensive Technol.*, Belgrade, Serbia, 2012, pp. 18–19.

[227] R. Austin, *Unmanned Aircraft Systems: UAVS Design, Development and Deployment*. Hoboken, NJ, USA: Wiley, 2011.

[228] M. Hassanalian and A. Abdelkefi, "Classifications, applications, and design challenges of drones: A review," *Progr. Aerosp. Sci.*, vol. 91, pp. 99–131, May 2017.

[229] K. Ro, W. Park, T. Kuk, and J. Kamman, "Flight testing of a free-wing tilt-body aircraft," in *Proc. AIAA Infotech@Aerospace*, 2010, p. 3449.

[230] Skybrary. *Helicopter Rotor Systems Configuration—SKYbrary Aviation Safety*. Accessed: Jul. 16, 2021. [Online]. Available: https://www.skybrary.aero/index.php/Helicopter_Rotor_Systems_Configuration

[231] J. S. Cook and J. S. Cook. (Mar. 31, 2015). 4 taxidermy drones: Yes, that's a thing. Makezine. Accessed: Jul. 16, 2021. [Online]. Available: http://www.makezine.com/2015/03/31/4-taxidermy-drones-yes-thats-thing

[232] H. Sato and M. M. Maharbiz, "Recent developments in the remote radio control of insect flight," *Frontiers Neurosci.*, vol. 4, p. 199, Dec. 2010.

[233] M. Baker and J. Manweiler, "Drones, robots, and sushi!" *IEEE Pervas. Comput.*, vol. 15, no. 1, p. 92-c3, Jan./Mar. 2016.

[234] L. S. Vailshery. (Mar. 8, 2021). IoT and non-IoT connections worldwide 2010–2025. Statista. Accessed: Jul. 15, 2021. [Online]. Available: https://www.statista.com/statistics/1101442/iot-number-of-connected-devices-worldwide/

[235] C. Rani, H. Modares, R. Sriram, D. Mikulski, and F. L. Lewis, "Security of unmanned aerial vehicle systems against cyber-physical attacks," *J. Defense Model. Simul.*, vol. 13, no. 3, pp. 331–342, Jul. 2016.

[236] P. Álvares, L. Silva, and N. Magaia, "Blockchain-based solutions for UAV-assisted connected vehicle networks in smart cities: A review, open issues, and future perspectives," *Telecom*, vol. 2, no. 1, pp. 108–140, Mar. 2021.

[237] M. Aloqaily, O. Bouachir, A. Boukerche, and I. A. Ridhawi, "Design guidelines for blockchain-assisted 5G-UAV networks," *IEEE Netw.*, vol. 35, no. 1, pp. 64–71, Jan./Feb. 2021.

[238] S. H. Alsamhi, B. Lee, M. Guizani, N. Kumar, Y. Qiao, and X. Liu, "Blockchain for decentralized multi-drone to combat COVID-19 and future pandemics: Framework and proposed solutions," *Trans. Emerg. Telecommun. Technol.*, vol. 32, no. 9, p. e4255, Sep. 2021.
[239] M. G. Santos De Campos, C. P. C. Chanel, C. Chauffaut, and J. Lacan, "Towards a blockchain-based multi-UAV surveillance system," *Frontiers Robot. AI*, vol. 8, Jun. 2021, Art. no. 557692.
[240] G. S. S. Chalapathi, V. Chamola, A. Vaish, and R. Buyya, "Industrial Internet of Things (IIoT) applications of edge and fog computing: A review and future directions," in *Fog/Edge Computing for Security, Privacy, and Applications*. Cham, Switzerland: Springer, 2021, pp. 293–325.
[241] G. K. Verma, B. B. Singh, N. Kumar, and V. Chamola, "CB-CAS: Certificate-based efficient signature scheme with compact aggregation for industrial Internet of Things environment," *IEEE Internet Things J.*, vol. 7, no. 4, pp. 2563–2572, Apr. 2020.
[242] Y. Zhu, G. Zheng, and K.-K. Wong, "Blockchain-empowered decentralized storage in air-to-ground industrial networks," *IEEE Trans. Ind. Informat.*, vol. 15, no. 6, pp. 3593–3601, Jun. 2019.
[243] Y. Dai, D. Xu, S. Maharjan, Z. Chen, Q. He, and Y. Zhang, "Blockchain and deep reinforcement learning empowered intelligent 5G beyond," *IEEE Netw.*, vol. 33, no. 3, pp. 10–17, May/Jun. 2019.
[244] A. Nanda, D. Puthal, J. J. P. C. Rodrigues, and S. A. Kozlov, "Internet of autonomous vehicles communications security: Overview, issues, and directions," *IEEE Wireless Commun.*, vol. 26, no. 4, pp. 60–65, Aug. 2019, doi: 10.1109/MWC.2019.1800503.
[245] H. Khelifi, S. Luo, B. Nour, H. Moungla, and S. H. Ahmed, "Reputation-based blockchain for secure NDN caching in vehicular networks," in *Proc. IEEE Conf. Standards Commun. Netw. (CSCN)*, Oct. 2018, pp. 1–6, doi: 10.1109/CSCN.2018.8581849.
[246] M. Li, J. Weng, A. Yang, J. Liu, and X. Lin, "Toward blockchain-based fair and anonymous ad dissemination in vehicular networks," *IEEE Trans. Veh. Technol.*, vol. 68, no. 11, pp. 11248–11259, Nov. 2019, doi: 10.1109/TVT.2019.2940148.
[247] R. Shrestha and S. Y. Nam, "Regional blockchain for vehicular networks to prevent 51% attacks," *IEEE Access*, vol. 7, pp. 95033–95045, 2019, doi: 10.1109/ACCESS.2019.2928753.
[248] Z. Yang, K. Yang, L. Lei, K. Zheng, and V. C. M. Leung, "Blockchain-based decentralized trust management in vehicular networks," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 1495–1505, Apr. 2019, doi: 10.1109/JIOT.2018.2836144.
[249] M. Dibaei, X. Zheng, Y. Xia, X. Xu, A. Jolfaei, A. K. Bashir, U. Tariq, D. Yu, and A. V. Vasilakos, "Investigating the prospect of leveraging blockchain and machine learning to secure vehicular networks: A survey," *IEEE Trans. Intell. Transp. Syst.*, early access, Aug. 20, 2021, doi: 10.1109/TITS.2020.3019101.
[250] *Aruba Marketing, 10 Blockchain and New Age Security Attacks You Should Know*. Accessed: Sep. 8, 2021. [Online]. Available: https://blogs.arubanetworks.com/solutions/10-blockchain-and-new-age-security-attacks-you-should-know/
[251] M. A. Cheema, M. K. Shehzad, H. K. Qureshi, S. A. Hassan, and H. Jung, "A drone-aided blockchain-based smart vehicular network," *IEEE Trans. Intell. Transp. Syst.*, vol. 22, no. 7, pp. 4160–4170, Jul. 2021, doi: 10.1109/TITS.2020.3019246.
[252] S. Guo, X. Hu, Z. Zhou, X. Wang, F. Qi, and L. Gao, "Trust access authentication in vehicular network based on blockchain," *China Commun.*, vol. 16, no. 6, pp. 18–30, Jun. 2019, doi: 10.23919/JCC.2019.06.002.
[253] M. A. Ferrag, M. Derdour, M. Mukherjee, A. Derhab, L. Maglaras, and H. Janicke, "Blockchain technologies for the Internet of Things: Research issues and challenges," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 2188–2204, Apr. 2019, doi: 10.1109/JIOT.2018.2882794.
[254] Z. Lu, Q. Wang, G. Qu, and Z. Liu, "BARS: A blockchain-based anonymous reputation system for trust management in VANETs," in *Proc. 17th IEEE Int. Conf. Trust, Secur. Privacy Comput. Commun./12th IEEE Int. Conf. Big Data Sci. Eng. (TrustCom/BigDataSE)*, Aug. 2018, pp. 98–103, doi: 10.1109/TrustCom/BigDataSE.2018.00025.
[255] U. Javaid, M. N. Aman, and B. Sikdar, "DrivMan: Driving trust management and data sharing in VANETs with blockchain and smart contracts," in *Proc. IEEE 89th Veh. Technol. Conf. (VTC-Spring)*, Apr. 2019, pp. 1–5, doi: 10.1109/VTCSpring.2019.8746499.
[256] X. Liu, H. Huang, F. Xiao, and Z. Ma, "A blockchain-based trust management with conditional privacy-preserving announcement scheme for VANETs," *IEEE Internet Things J.*, vol. 7, no. 5, pp. 4101–4112, May 2020, doi: 10.1109/JIOT.2019.2957421.
[257] C. Zhang, W. Li, Y. Luo, and Y. Hu, "AIT: An AI-enabled trust management system for vehicular networks using blockchain technology," *IEEE Internet Things J.*, vol. 8, no. 5, pp. 3157–3169, Mar. 2021, doi: 10.1109/JIOT.2020.3044296.
[258] P. K. Singh, R. Singh, S. K. Nandi, K. Z. Ghafoor, D. B. Rawat, and S. Nandi, "Blockchain-based adaptive trust management in internet of vehicles using smart contract," *IEEE Trans. Intell. Transp. Syst.*, vol. 22, no. 6, pp. 3616–3630, Jun. 2021, doi: 10.1109/TITS.2020.3004041.
[259] B. Li, R. Liang, D. Zhu, W. Chen, and Q. Lin, "Blockchain-based trust management model for location privacy preserving in VANET," *IEEE Trans. Intell. Transp. Syst.*, vol. 22, no. 6, pp. 3765–3775, Jun. 2021, doi: 10.1109/TITS.2020.3035869.
[260] Y. Teng, Y. Cao, M. Liu, R. Yu, and V. C. M. Leung, "Efficient blockchain-enabled large scale parked vehicular computing with green energy supply," *IEEE Trans. Veh. Technol.*, early access, Jul. 26, 2021, doi: 10.1109/TVT.2021.3099306.
[261] M. Kamal, G. Srivastava, and M. Tariq, "Blockchain-based lightweight and secured V2V communication in the internet of vehicles," *IEEE Trans. Intell. Transp. Syst.*, vol. 22, no. 7, pp. 3997–4004, Jul. 2021, doi: 10.1109/TITS.2020.3002462.
[262] M. Cebe, E. Erdin, K. Akkaya, H. Aksu, and S. Uluagac, "Block4Forensic: An integrated lightweight blockchain framework for forensics applications of connected vehicles," *IEEE Commun. Mag.*, vol. 56, no. 10, pp. 50–57, Oct. 2018, doi: 10.1109/MCOM.2018.1800137.
[263] Y. Yao, X. Chang, J. Mišić, V. B. Mišić, and L. Li, "BLA: Blockchain-assisted lightweight anonymous authentication for distributed vehicular fog services," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 3775–3784, Apr. 2019, doi: 10.1109/JIOT.2019.2892009.
[264] (Apr. 2018). *Autonomous Car Crashes: Who-Or What-is to Blame?* Accessed: Jun. 9, 2021. [Online]. Available: https://knowledge.wharton.upenn.edu/article/automated-car-accidents/

SAURABH JAIN received the master's degree (M.Tech.) in information security from MANIT, Bhopal, Madhya Pradesh, India, in 2012. He is currently pursuing the Ph.D. degree in CSE with the University of Petroleum and Energy Studies, Dehradun, India. He has worked as an Assistant Professor with the Department of CSE, Oriental College of Technology, Bhopal, where he has worked as the HOD, a M.Tech. Coordinator, and a Remote Center Coordinator, in the past. He is working as an Assistant Professor with the School of Computer Science, University of Petroleum and Energy Studies. He has published more than 30 international research papers and patents. He has conducted many international/national conferences, workshops, FDPs, and STPs. He was a Certified Quick Heal Academy Certified Cyber Security Professional (QCSP), in 2018. His research interests include network security, web security, cryptography, and blockchain technology.

NEELU JYOTHI AHUJA received the Ph.D. degree, in 2010.

Her Ph.D. thesis was about developing a prototype rule-based expert system for seismic data interpretation. She is currently a Professor and the Head of the Department of Systemics, School of Computer Science, University of Petroleum and Energy Studies, Dehradun. Apart from academic teaching at the university level (both post-graduate and under-graduate), she is an Active Researcher. From 2010 to 2017, she was the Head of spearheading intra-disciplinary research and coordinating research activities with the Research Centre-Computing Research Institute. She has successfully delivered and is executing government sponsored research and development projects from the Department of Science and Technology (DST). She has completed one research and development project funded by Uttarakhand State Council for Science and Technology (UCOST, Dehradun) and two [one from Cognitive Science Research Initiative (CSRI) Division and one from Science for Equity, Empowerment, and Development (SEED)] Divisions of DST. She is executing a research and development project sponsored by the Science for Equity, Empowerment, and Development (SEED) Division of DST under their Technology Intervention for Disabled and Elderly (TIDE). She also holds successful conduction of DST-funded consultancies to her credit. Under her supervision, five Ph.D. scholars have been awarded. Six research scholars are undergoing their Ph.D. work under her supervision. She holds more than 20 years of experience in teaching, research, and

project proposal development. She has published papers in journals and conferences at the international and national levels. Her research interests include machine learning, intelligent systems, intelligent tutoring systems, expert systems, artificial intelligence, ICT, object-oriented development, and programming languages.

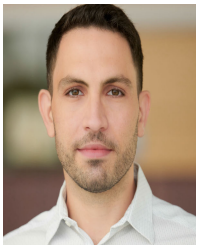
Prof. Ahuja has been an invited speaker on various technical and research-oriented topics at widely acclaimed forums, both national and international. She is on the panel of multiple committees, including WHO-Promotion of Assistive Products and Technologies and DST-Expert Committee for inspection and on-the-spot review of CORE (long-term) projects. She has been the chair at various conference sessions and different internal and external meetings/forums.

P. SRIKANTH received the B.Tech. degree in information technology and the master's degree (M.Tech.) in computer science with specialization in parallel computing from JNTU Hyderabad, India, in 2006 and 2012, respectively. He is currently an Assistant Professor-Selection Grade with the School of Computer Science, University of Petroleum and Energy Studies, Dehradun, India. His main research interests include trust assessment, social networks, information security, and mobile *ad-hoc* networks. Many of his research publications have appeared in reputed journals, conferences, and workshops.

KISHOR VINAYAK BHADANE received the Ph.D. degree in electrical engineering from RTM Nagpur University, under the guidance of Dr. M. S. Ballal, a Professor with the Electrical Department, V.N.I.T., Nagpur. He is currently working as an Associate Professor with the Electrical Engineering Department, Amrutvahini College of Engineering, Sangamner, Maharashtra, India. He has a total of 18.5 years of experience in teaching. He has 39 publications to his credit in reputed international journals, like SCI, SCOPUS Indexed, and conferences. He has two Indian and two Australian patent on his research. He has successfully handled the responsibility of Dean, Academics, and Dean, Projects. Under this portfolio, he has successfully collaborated with more than 20 industries in the area of industry problems research with the help of III activities, like GIZ Germany and NIMA Nashik. His research interests include power quality, renewable energy, wind energy, custom power devices, electric vehicles, grid integration issues, grid codes, research and funding, and industry institute interaction (III). He was a recipient of various government and non-government organizations, such as AICTE, NMU, RGI, GIZ Germany, DST, EDII, Ministry Skill Development, and Bosch International Training Center, approximately Rs. 80 Lakhs. He is a Reviewer of IEEE Transactions on Power Electronics, IEEE Transactions on Industrial Electronics, IEEE Transactions on Smart Grid, *RSER* (Elsevier), and *IET* (Springer).

BHARATHRAM NAGAIAH received the B.Tech. degree in petrochemical technology from Anna University (formerly known as the School of Engineering and Technology), Tiruchirappalli, India. During his experience, he played architect roles in different areas, such as digital transformations, business transformation, supply chain operations, technology implementations, and enterprise architecture. He is an industry professional in global supply chain systems and operations for almost 18 years and is currently based in USA. He has worked in multiple verticals, including oil and gas, high tech, industrial manufacturing, life science and healthcare, telecom, and consumer products. He has designed and delivered business systems for customer service, manufacturing, and supply chain domains with a unique strategy, enterprise structure, and innovative solutions. He has contributed to various seminars on ERP technologies at different forums and has actively contributed to developing interoperability standards for the SMART Manufacturing Community.

ADARSH KUMAR received the M.Tech. degree in software engineering from Thapar University, Patiala, Punjab, India, and the Ph.D. degree from Jaypee Institute of Information Technology, Noida, Uttar Pradesh, India. He held a postdoctoral position with the Software Research Institute, Athlone Institute of Technology, Ireland. From 2005 to 2016, he was associated with the Department of Computer Science Engineering and Information Technology, Jaypee Institute of Information Technology, where he worked as an Assistant Professor. He is currently an Associate Professor with the School of Computer Science, University of Petroleum and Energy Studies, Dehradun, India. He has participated in European Union H2020 Sponsored Research Project and is executing two research projects sponsored by the UPES SEED Division and one sponsored by Lancaster University. He has many research papers in reputed journals, conferences, and workshops. His main research interests include cybersecurity, cryptography, network security, and *ad-hoc* networks.



CHARALAMBOS KONSTANTINOU (Senior Member, IEEE) received the M.Eng. degree in electrical and computer engineering from the National Technical University of Athens (NTUA), Greece, in 2012, and the Ph.D. degree in electrical engineering from New York University (NYU), NY, USA, in 2018. He is currently an Assistant Professor of computer science (CS) and an Affiliate Professor of electrical and computer engineering (ECE) with the Division of Computer, Electrical, and Mathematical Science and Engineering (CEMSE), King Abdullah University of Science and Technology (KAUST), Thuwal, Saudi Arabia. He is also the Principal Investigator of the Secure Next Generation Resilient Systems Lab (SENTRY) and a member of the Resilient Computing and Cybersecurity Center (RC3), KAUST. Before joining KAUST in the Summer of 2021, he was an Assistant Professor with the Center for Advanced Power Systems (CAPS), Florida State University (FSU), from 2018 to 2021. He has authored multiple articles in the ACM/IEEE Transactions and conference proceedings. His research interests include secure, trustworthy, and resilient cyber-physical and embedded IoT systems. He is also interested in critical infrastructures security and resilience with a particular focus on smart grid technologies, renewable energy integration, and real-time simulation. He is a member of ACM and an ACM Distinguished Speaker, for the period 2021–2024. He serves in the program committee for several international conferences. He was a recipient of the 2020 Myron Zucker Student-Faculty Grant Award from the IEEE Foundation, the Southeastern Center for Electrical Engineering Education (SCEEE) Young Faculty Development Award 2019, and the Best Paper Award at the International Conference on Very Large Scale Integration (VLSI-SoC) 2018. He is the Chair of the IEEE Task Force on Resilient and Secure Large-Scale Energy Internet Systems and the Secretary of the IEEE Task Force on Cyber-Physical Interdependence for Power System Operation and Control. He serves as an (Guest) Associate Editor for the *International Journal of Electrical Power and Energy Systems*, *Computer* (IEEE), *IET Generation, Transmission and Distribution*, and *IEEE Consumers Electronics Magazine*.