Review

Applications of Blockchain and Smart Contracts to address challenges of Cooperative, Connected and Automated Mobility

Christos N Kontos , Theodor Panagiotakopoulos * , Achilles Kameas

Posted Date: 5 July 2024

doi: 10.20944/preprints202407.0493.v1

Keywords: Cooperative; Connected and Automated Mobility; Blockchain; Smart Contracts; Internet of Things; Internet of Vehicles

Review

Applications of Blockchain and Smart Contracts to Address Challenges of Cooperative, Connected and Automated Mobility

Christos Kontos [1], Theodor Panagiotakopoulos [1,2,*] and Achilles Kameas [1]

[1] School of Science and Technology, Hellenic Open University, 18 Parodos Aristotelous street, 26335 Patras, Greece; kontoschr@gmail.com (C.K.); kameas@eap.gr (A.K.)
[2] Business School, University of Nicosia, 46 Makedonitissis Street, 2417, Nicosia, Cyprus
* Correspondence: panagiotakopoulos@eap.gr

Abstract: Transportation plays an important role in urban development. Population growth and environmental burden have turned the efforts of cities globally towards smarter and greener mobility. Cooperative and Connected Automated Mobility (CCAM) serves as a concept with the power and potential to help achieve these goals building upon technological fields like Internet of Things, computer vision and distributed computing. However, its implementation is hindered by various challenges covering technical parameters such as performance and reliability in tandem with other issues, such as safety, accountability and trust. To overcome these issues, new distributed and decentralized approaches like blockchain and smart contracts are needed. This paper aims at identifying a comprehensive inventory of CCAM challenges and use it as a framework to describe methodologies using blockchain and smart contracts to address them. It provides a comparative analysis of the findings to draw useful conclusions and discuss future directions in CCAM and relevant blockchain applications. The paper contributes to intelligent transportation systems' research by offering an integrated view of the difficulties in substantiating CCAM and providing insights on the most prominent blockchain and smart contract technologies that tackle them.

Keywords: cooperative; connected and automated mobility; blockchain; smart contracts; internet of things; internet of vehicles

1. Introduction

The constantly growing population in urban settlements is the source of many problems for their citizens such as heavy traffic, long commuting times, air and noise pollution, expansion of transport infrastructure and increase in vehicles [1]. In recent years, the spread of advanced technologies and especially the integration of Internet of Things (IoT) in urban transportation infrastructures, allowed the development of smarter and greener mobility systems and applications. Smart mobility is an umbrella term used to describe and promote the disruptive changes in the transport sector related to the automation, digitalization and economics of transport infrastructure [2].

Smart and green mobility has three goals [3]: sustainability, safety and cost-effectiveness. In order to achieve these objectives, it encompasses a rich variety of innovative IoT-driven solutions: smart parking systems, smart logistics, shared mobility, integrated ticketing systems, route optimization, autonomous driving, smart payment systems, cooperative vehicle awareness, route optimization, traffic management, accident detection and, road anomalies detection [1,4–6].

One of the most prominent emerging application areas of smart mobility is Cooperative, Connected and Automated Mobility (CCAM), which allows vehicles to interact with each other and transportation infrastructures enabling real-time data collection and analysis for coordinated action [7]. It has generated significant attention among researchers, industry and governments as it is expected to unveil disruptive opportunities for societies and economies [8]. Connected and

 doi:10.20944/preprints202407.0493.v1

Automated vehicles (CAVs) have the ability to address traffic congestion in a cooperative manner [9] and the potential to remove risk factors associated with human driving errors and therefore to reduce the number of road accidents, while improving the functionality of transport systems [10].

However, safe and reliable operation of CAVs still needs considerable progress, testing for building acceptance and trust and regulatory approval for their commercial availability [11]. In order to deliver on their promise, CAVs need to overcome a range of shortcomings and limitations, such as those related with currently used sensing technologies [12] and centralized computing architectures [13]. This is exacerbated by the complexity and scale of vehicular IoT networks, which make the application of CCAM in smart cities more difficult and hinder large-scale urban deployments. On the other hand, various scholars argue that technological issues of CCAM create important ethical, legal, and societal considerations (e.g., [14]). To overcome these issues, new technologies are explored based on distributed and decentralized approaches. Towards this direction, the emergence of blockchain technologies and smart contracts has brought a key enabler of distributed information systems and IoT infrastructures in urban transportation.

The process of selecting/developing and applying appropriate blockchain and smart contracts mechanisms in CCAM solutions predominantly relies on the challenge that needs to be solved. Although several works present important challenges of CCAM and propose blockchain-based and other mechanisms to deal with them, an inclusive taxonomy is still missing. This is because these challenges are examined from specific perspectives directly related to different applications of autonomous driving in smart cities. To fill this gap, our work aims to piece together a more comprehensive understanding of CCAM challenges by drawing up a detailed inventory of theirs and build on this to explore the most prominent blockchain and smart contracts mechanisms to address them. Table 1 displays recent surveys on CCAM challenges and demonstrates the novelty of our paper.

Table 1. Comparison of relevant surveys.

Survey	Technical Challenges	Social Challenges	Ethical Challenges	Blockchain approaches
[12,15,16]	✓			
[13]	✓			✓
[14,17,18]		✓	✓	
[19]			✓	
[20]	✓		✓	
This work	✓	✓	✓	✓

The contribution of this work is threefold. First, it presents a comprehensive list of CCAM challenges classified into three categories: technical, social, and ethical (see Table 1). In addition, the importance of these challenges and the impact they have in the acceptance of CCAM in mobility is discussed. Second, it identifies existing methodologies and solutions to address these challenges based on blockchain and smart contracts. Third, we make a critical review of these methodologies eliciting qualitative and quantitate features to create a framework for comparing different methods' performance for each challenge.

2. Background

The purpose of this section is to present the background knowledge around the basic building blocks of this work.

 doi:10.20944/preprints202407.0493.v1

2.1. Vehicular Ad-Hoc Networks and CCAM

Vehicular Ad-hoc Networks (VANETs) are a subclass of unstructured Mobile Ad-hoc Networks (MANETs) in which the nodes of the network are the vehicles that communicate both with each other and with the base stations [21]. The vehicles participate in the network either as routers or as wireless access points and move continuously. They support three types of communication: in-vehicle communication, unstructured communication with other vehicles and with base stations (ad-hoc) and infrastructure communications (infrastructural) [22].

The nodes in VANETS are located exclusively on vehicles and their topology is very dynamic. Their routes are mostly predefined as the vehicles move exclusively on the road network [23]. Vehicles have varied capabilities in terms of processing power, autonomy (energy supply) and data storage but they require a continuous supply of high bandwidth for efficient operation [24]. These nodes move at very high speeds and change their position instantaneously and continuously. At the same time, their connection to both the neighboring vehicles and the central network is interrupted and connected continuously.

The VANETs are also a subnetwork of Internet of Vehicles (IoV) since the latter contain other networks such as the communication network of infrastructures with each other and with the internet and finally the interconnection of all those involved in smart mobility, people, vehicles, things and the road environment. According to [21], applications of VANETs in smart mobility are divided into 2 categories:

- Safety applications: collision avoidance, curve speed warning, traffic signal violation, emergency brake lights, pre-collision detection, collision warning, left turn assist, lane change warning.
- Non-safety applications: traffic information, infotainment applications, weather and points of interest information.

The architecture of VANETs consists of three domains: mobile, infrastructure and general domain [21]. The mobile domain includes the vehicles with their On-Board Units (OBUs), Mobile Units (MUs) and Application Units (AUs). Roadside Units (RSUs) are network components that are usually located at fixed points along the sides of the road or at specific locations [25]. The RSUs along with the sensors of a smart city, belong to the infrastructure domain. The general domain contains the internet access and some private infrastructure like SaaS or IaaS providers or content providers. The architecture of VANETs provides communications between mobile nodes (vehicles) and fixed points located along a road [26]. There are two categories of communications [27]:

- Mobile communications: In-Vehicle and Vehicle-to-Vehicle (V2V)
- Fixed node communications: Vehicle-to-Infrastructure (V2I) and Vehicle-to-Broadband Cloud (V2B or V2C)

2.2. Blockchain Fundamentals

Blockchain first appeared in 2008 bringing new and unique features to the IT and internet world that were not possible before such as reliable decentralized information systems without the mediation of a central authority [28]. The original idea was to store in a file called block, the data of the transactions as well as the code of the previous transaction along with a timestamp. Each new block was linked to the previous one using cryptographic techniques, thus forming a chain of blocks. The motivation was to create a digital or virtual currency that would maintain its value without the involvement of any financial or banking central entity. But the key technology that started from his work and that has caught the interest of the research world in the field of IT while at the same time transforming the business world is Blockchain.

Blockchain is a chain of transactions in which each transaction is related to the previous last transaction. The unique id of each block is a hash which is created using the hashing algorithm with 256-bit encryption (SHA256) and which is applied to the header of the block. A key feature of this algorithm is that knowing its output, one cannot discover the original data before encryption, while the more possible hashes, the less chance there is of two values creating the same hash value [29].

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 5 July 2024 doi:10.20944/preprints202407.0493.v1

Blockchain is a pervasive network consisting of computer nodes connected to the Internet that together maintain an account of transactions performed on the network. A record of each transaction is shared throughout the network while the approval of the transaction is not done by a central system but by a group of computers participating in the network. These records, which are called blocks, are part of a chain of blocks (blockchain) and each of them is related (referenced) to the previous block. Looking at transportation and CCAM (Figure 1), blockchain has been used in a rich variety of applications, such as forensics [30], sensor security [31] and collective intelligence protection [32].

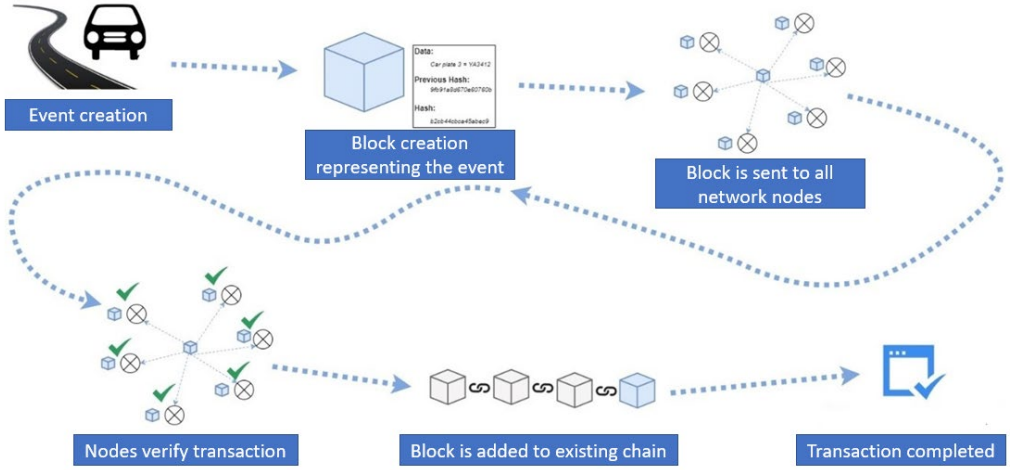

Figure 1. The stages of creating and adding a new block.

2.3. Smart Contracts

A division in blockchain technology based on two transaction models, the token-based model and the account-based model is presented in [13]. Smart contracts belong to the second model and are placed in the second stage of Blockchain development called Blockchain 2.0.

The general definition of smart contracts states that a smart contract consists of a computer program that can automatically execute and apply the terms of a contract [33]. More specifically, a smart contract refers to a computational transaction protocol that executes the terms of a contract, satisfying common contractual terms such as payment, retention, confidentiality, enforcement of an agreement while at the same time minimizing malicious or accidental disputes as well as the need for trusted intermediaries [34]. Smart contracts are self-executing and incorporate the ownership information of assets, thus overcoming the problem of counterparty trust [35]. By assets we do not necessarily mean coins but any asset that can be digitized. Thus, we observe that the use of smart contracts as digital money protocols can be applied not only to money but also to a wide variety of digital assets [36]. According to the transactions carried out through conventional financial organizations, many techniques are needed for a payment to be safe and guaranteed, such as live contact, certified mail, credibility of the contracting party's credit history, etc. Smart contracts go beyond the above techniques, providing transparency, reliability, and cost reduction due to both the elimination of fraud and the observance of agreements (guarantees) [37].

Smart contracts can help eliminate the need for intermediaries, such as banks or legal professionals, in many types of transactions. They can also increase efficiency, reduce costs, and improve security by eliminating the need for human intervention and reducing the risk of fraud or error [38]. Because smart contracts are stored on a decentralized blockchain, they are immutable and transparent, meaning that once a smart contract is deployed, it cannot be altered or tampered with (Figure 2). This makes smart contracts a secure and trustworthy way to conduct transactions and enforce agreements between parties.

 doi:10.20944/preprints202407.0493.v1

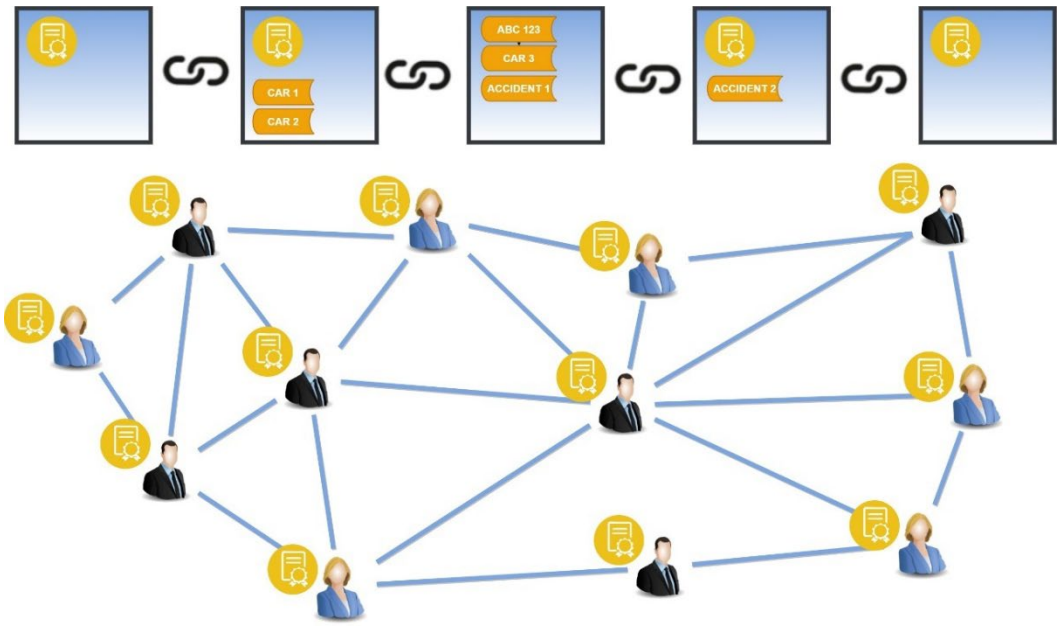

Figure 2. A smart contract is based on blockchain technology.

Smart contracts work through four steps [39]. In the first step, the contracting parties should determine the terms of the contract (payment, retention, confidentiality, etc.) as well as the conditions of execution such as the time of execution. Then once the contractual terms are agreed and finalized, they are converted into programming code. In the second step, the execution of the contract is activated. Execution is triggered by either an event such as an initialization transaction or the collection of information appropriate for the execution of the contract. In the third step, the code of the contract is executed by all the nodes of the network and if any condition of the contract is satisfied and verified by all the participating nodes of the blockchain network, then the values are transferred according to the initial conditions of the contract. In the fourth step, the agreement (settlement) is performed or the liquidation of the elements that are on the chain such as for example digital currencies. However, in the case of off-chain items such as shares or cash, then their respective accounts are updated

3. Method

3.1. Research Questions

Based on the research objectives of our study, we formulated the following research questions to examine what current literature includes on CCAM challenges and related mechanisms to address them based on blockchain and smart contracts.

RQ1: Which are the most important challenges of CCAM and how can they be classified?

RQ2: Which solutions utilizing blockchain technologies and smart contracts are used in response of CCAM challenges?

RQ3: How does each blockchain and/or smart contract method performs and which are its pros and cons?

3.1. Research Methodology

We followed a Systematic Literature Review (SLR) approach [40] using well-specified methods to identify, screen and eventually select research articles directly connected to our study's research questions. We employed the PRISMA model for our SLR [41], which was conducted at two phases.

The first phase focused on the challenges of CCAM. Several well-known electronic scientific databases were queried for the literature review. In order to enhance the credibility and integrity of the study, exclusively peer-reviewed journal or conference papers were taken under consideration.

 doi:10.20944/preprints202407.0493.v1

We searched the following scientific databases: IEEE Xplore, Science Direct, and Scopus by using the string ("Cooperative" AND "Connected" AND "Autonomous" AND "Vehicles" AND "Challenges"). We also limited publication date between 2018 and 2023. A total of 139 unique articles from the search were screened and assessed based on the title and abstract. We excluded duplicates and non-peer-reviewed journal or conference articles and articles not focusing on surveys about CCAM challenges, reducing the number of relevant articles to 10 (Figure 3). The selected papers were downloaded and read in full. Based on the articles included in our SLR, we elicited 12 major CCAM challenges and categorized them in technical, social, and ethical challenges.

The second phase consists of the literature review for methods that deal with the above challenges in CCAM with the application of blockchain and smart contracts. For the identification of articles addressing this topic, we searched for articles in the same three databases. Our search string was ("VANET" OR "Vehicular Networks" OR ("Cooperative" AND "Connected" AND "Autonomous" AND "Vehicles") AND "blockchain" OR "smart contract" AND "name of each CCAM challenge") and we performed 12 searches, one for each CCAM challenge. We excluded duplicates and non-peer-reviewed journal or conference articles and articles, as well as articles not providing empirical data, such as abstracts, editorials, conference summaries, short papers, and book chapters. It is important to mention that our search revealed several articles employing similar methods. In such cases, we included only one article per method in our study, based on the extent of technical details, and the existence of a case study and evaluation. All non-English written articles were also excluded. 19 articles met these criteria, as shown in Figure 3. We studied the full texts of these articles and conducted a further backward reference search to learn more about this body of knowledge development.

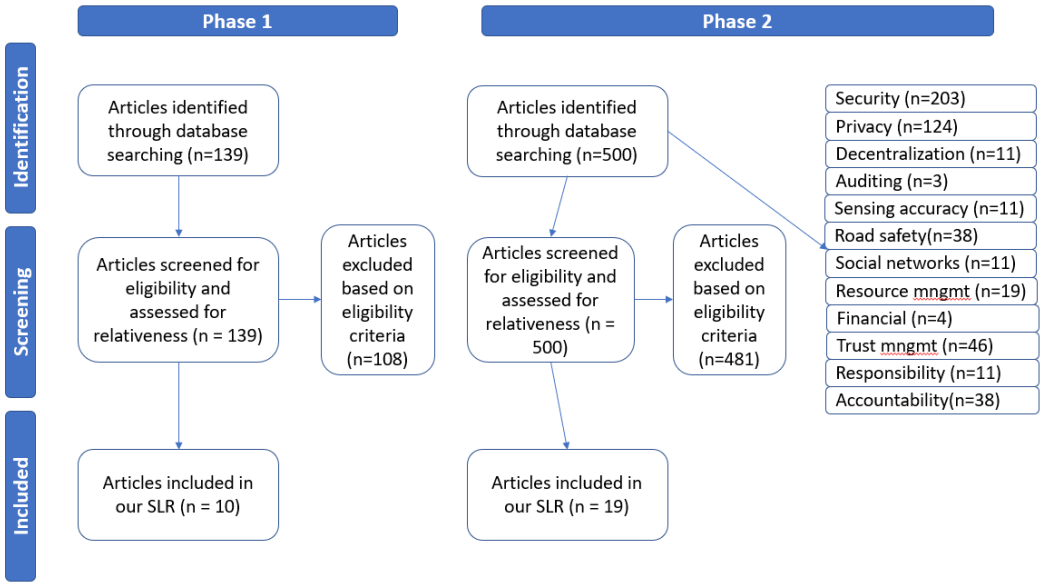

Figure 3. PRISMA review process.

4. Taxonomy of Challenges in CCAM

Autonomous and connected vehicles have significant shortcomings and limitations as well as challenges. For example, autonomous vehicles have limitations in sensing technologies that are not reliable in particular weather and road conditions. Furthermore, integrated AI systems function as a "black box" without a clear explanation of how they work. On the other hand, connected vehicle technologies are completely dependent on messaging to achieve mutual understanding, which will have a big impact when the former gain a lot of penetration on the streets of smart cities [12].

Based on the relevant literature, we identified twelve (12) major challenges in CCAM classified in three categories: technical, social, and ethical (Figure 4).

 doi:10.20944/preprints202407.0493.v1

Figure 4. The taxonomy of challenges in CCAM.

4.1. Technical Challenges

Security: Security of data and messages exchanged between vehicles and with RSUs and central infrastructures. Information security and cybersecurity issues such as issues of availability, data integrity, confidentiality, authenticity, and the corresponding attacks.

Privacy: Protection of the data of the involved parties of the road network. Avoid disclosing their true details to third parties. Identity management of vehicles and passengers.

Decentralization: Protection of VANETs from the failure of centralized infrastructures and design of road systems without centralized control and centralized storage of data and messages. Mechanisms that allow free connection and exchange of data between nodes.

Auditing: Logging of data, messages, and events both locally and remotely with integrity and speed, enabling access to all authorized stakeholders in VANETs.

Sensing Accuracy: Mechanisms to improve the accuracy of vehicle sensors to provide valid and actionable vehicle movement, traffic, and state data.

4.2. Social Challenges

Road safety: The road network should provide safety to both vehicle passengers and pedestrians, thus increasing citizens' trust in the CCAM.

Social Networks: New types of data exchange between vehicle passengers and the rest of the network as well as continuous access to the internet is a challenge for CCAM and VANET networks.

Resource management: The distribution of resources in processing, storage and communications is a challenge for the road network and for its nodes (fixed or mobile)

Economy: Techniques and methods to ensure a more cost-efficient use of VANET networks which will help in their green implementation.

 doi:10.20944/preprints202407.0493.v1

4.3. Ethical Challenges

Trust management: Improving the reliability and safety of autonomous and interconnected vehicles creates such conditions as to increase people's trust. Trust is a major challenge of CCAM and VANETs.

Responsibility: Methodologies which will protect the road system from avoiding blaming an accident or incident on the vehicle that causes it.

Accountability: Techniques which record and assign the events to the respective vehicles that cause them without raising issues of the privacy of the users and passengers of the road network.

5. Blockchain and Smart Contract Approaches for CCAM Challenges

5.1. Approaches for Technical Challenges

The sharing of data between mobile nodes (vehicles) and fixed nodes (RSUs) as well as their storage in distributed storage, with security, reliability and protection against tampering and identity attacks, is the subject of discussion in [42]. To address the security issues in VANETs, the authors propose the DSSCB framework which is a new data security sharing and storage system based on blockchain consortium with Practical Byzantine Fault Tolerance (PBFT) consensus mechanism. This mechanism addresses the inefficiency of the original Byzantine fault-tolerant consensus algorithm and reduces the complexity of the algorithm, thus solving the problem of data loss and delay in conditions congestion while providing satisfactory error handling in VANET networks. The vehicles with the most frequent contributions, offer cooperative intelligence to VANETs and thus have more coins and higher priority to access the data collected locally by the RSUs.

The authors of [43] dealt with the geographical scope of VANETs and pointed out that each country maintains its own blockchain network based on Proof of Work (PoW) consensus mechanism which is limited to the geographical boundaries of the country. The aim of the paper is to describe its security risks and it specifically focuses on the 51% attack or majority attack, which can undermine the immutability of blockchain technology. The probability is also analyzed under specific parameters such as the number of "good" and "bad" nodes, the propagation time of the messages (delay), as well as the time to calculate the puzzle of the consensus mechanism. The authors define those parameters which ensure message transmission thus providing a set of guidelines for the design of similar systems.

Both security and privacy are issues to be resolved in VANETs. This is highlighted in [44], which is based on the implementation of the conditional privacy-preserving authentication (CPPA) protocol whose significant limitations and implementation problems are overcome using blockchain technology (BCPPA). Thus, a modified digital signature protocol, ECDSA, is proposed to perform group signature verification by vehicles and RSUs thereby minimizing the verification cost in VANETs. Certificates of transactions between vehicle OBUs and Certificate Authorities (CA) are stored in blockchain while Smart Contracts are used mainly to display the public key of vehicles with the identity of the transaction in the blockchain.

Focused on privacy in VANETs, [45] suggests a mechanism for issuing nicknames to vehicles as well as their management is proposed, based on PKI and permissioned blockchain & smart contracts technologies. The authors point out that blockchain technology alone cannot reliably guarantee authentication and nonrepudiation except with the combination of blockchain and PKI. In relation to pre-existing works, this particular methodology provides the possibility of collaboration between several authorities using the above technologies. For this purpose, the architecture is based on three main elements: the blockchain network which contains nodes (competent authorities, jurisdictions) in which smart contracts are executed, consensus services, authorization and authentication services, RSUs which are the connecting link between authorities for the certification of nicknames and vehicles and finally the local authorities which are parts of the state and are responsible for managing traffic and enforcing the law on the road network. The authors noted that the performance improvement needs further investigation if we consider that the work does not refer to the parallel and distributed execution of the operations by an RSU.

 doi:10.20944/preprints202407.0493.v1

Decentralization is addressed by methodologies that consider how to transmit the messages from the various events in the road network, without the mediation of a central infrastructure, while considering distributed processing and storage especially when nodes have resource constraints. In this direction, the authors in [46] propose a Proof-of-Quality-Factor (PoQF) consensus mechanism that runs in 4 phases and is based on multi-hop message relaying to vehicle mobile nodes for V2V communications. In this mechanism, a critical role is played by the signal-to-interference-noise ratio (SINR), which is the measure for the successful transmission of packets through multi-hop intermediate nodes. The use of polling determines the quality of the signal and thus the delay of the transmission of the packets. In this work, a comparison of the performance of the consensus mechanism with respect to the others is made through simulation, where it is found that it offers moderate performance in terms of security, low performance in terms of complexity in communications, but overall it is more efficient as the nodes increase, making it suitable for environments with large scale. Similarly

Collaborative location accuracy using Deep Neural Networks (DNN) and blockchain technology and smart contracts is examined in [47]. Aiming to identify the exact position of a vehicle, fixed reference points (landmarks) are used whose exact geographical position is known. With these fixed points, they calculate the errors from the geographical values of the mobile nodes and then train the neural networks according to the corrected data they collect. The corrected positions are stored in a blockchain through which the cooperative vehicles share them. All vehicles share them corrected positions without being revealed to external or internal attackers due to the decentralized and immutable nature of blockchain technology. The architecture of the methodology of [47] includes mobile edge computing nodes (MECs) that have storage space and processing power for blockchain operations and for Delegated Proof of State (DPoS) consensus mechanism but also for performing DNN operations. Both the recording of the location and its sharing between the MECs and the vehicles is done using smart contracts.

The methodology of [48] concerns the collection of the data from the vehicles and then sending them through the RSUs to the central servers of the road infrastructure in order to be controlled and used by all involved parties in the road network. For the safe transmission of data, blockchain technology is applied in which the data is encrypted based on the characteristics that concern it. Through the blockchain network vehicles can access and search for the information they want based on their own characteristics. This auditing procedure is done according to predefined and not dynamic policies. This is also a key drawback of the methodology. The consensus mechanism is based on the Proof-of-Storage mechanism according to which the RSUs with the largest storage contribution are rewarded with storage-coins. The authors analyze the performance of the methodology and point out that it is quite efficient compared to previous methodologies, but the time cost for the encryption and decryption operations is similar.

A summary of the discussed approaches towards technical challenges of CCAM, as well as their technical features are shown in Table 2 and Table 3 respectively.

Table 2. Blockchain and smart contract methodologies for technical CCAM challenges.

Ref	Challenge	Summary	Advantages	Disadvantages
[42]	Security	Protection mechanism against malicious attacks on the data collected by RSUs of VANET networks using blockchain technology for distributed data storage and smart contracts for access by vehicles and	Protection against attacks on centralized systems, due to the decentralized architecture. Protection against Brute Force attacks based on asymmetric encryption and	With a small number of involved RSUs in the network there is an increased possibility of malicious tampering and thus the system is unstable.

 doi:10.20944/preprints202407.0493.v1

	neighboring RSUs through data coins.	signature verification techniques. Protection against malicious RSUs.	
[43] Security	Description and configuration of secure message transmission in geographically defined blockchain systems in VANETs so that they are protected against majority attacks.	It defines those parameters that ensure the secure transmission of messages in VANETs located in a limited geographical area.	Even with a small percentage of malicious nodes, if the delay time of messages from malicious nodes is less than "good" nodes, the 51% attack is quite possible.
[44] Security	Protocol for creating secure communications in VANET networks based on the blockchain version of the conditional privacy-preserving authentication (CPPA) protocol	Provides security against various types of attacks such as: Hijacking, 51% resistance to attacks, DDoS, Man-in-the-middle	The average packet delay (APD) of the data is affected by changes in the average speed of the vehicles.
[45] Privacy	Protection against transmission of false messages in vehicle transactions in V2V & V2I communications based on authentication through blockchain technology	Efficient methodology because it reduces the dependency on the central authorization authority and the burden on vehicle authentication	It is not a purely decentralized solution because it is based on a relatively small number of servers in the cloud.
[46] Decentralization	Blockchain technology consensus mechanism based on node votes for road event transmission	Reliable mechanism in case of knotting. Fewer validation losses than other consensus mechanisms.	The voting mechanism causes long delays in the transmission of messages (latency). It is impervious to 51% majority attacks.
[47] Sensing Accuracy	A methodology that uses blockchain and smart contracts in combination with neural networks to improve location accuracy and share it in VANET networks	Improvement in position accuracy is possible even when access to reference points is interrupted	It does not consider random errors in positioning
[48] Audit	Mechanism for recording vehicle announcements based on quality characteristics, based on blockchain technology	It reduces the need for processing power in vehicles	Stored feature policies are not dynamic and do not change.

 doi:10.20944/preprints202407.0493.v1

Table 3. Technical features of blockchain and smart contracts' methodologies for technical CCAM challenges.

Ref Challenge	Blockchain / Smart Contract	Consensus mechanism	Techniques/tools	Performance of the methodology
[42] Security	Blockchain	PoW & Practical Byzantine fault tolerance (PBFT)	-	Better performance in computation and transmission times as the number of verification signatures increases, compared to existing solutions (IBV, SPRING, IBCPPA and EAAP)
[43] Security	Blockchain	PoW	-	It implements the BIP325 key extraction algorithm to avoid preloading keys and burdening OBUs with storage consumption. The performance of the technique is not affected by the average speed as far as packet loss is concerned
[44] Security	Permissionless Blockchain & Smart Contracts (Ethereum)	PoW & Proof-of-Stake	-	The methodology is efficient for small delay time in the transmission of messages from the group of "good" nodes
[45] Privacy	Blockchain	PoW	Distributed Cloud Servers	It achieves fewer cycles (steps) in communication compared to pre-existing methodologies
[46] Decentralization	Blockchain	Proof-of-Quality-Factor (PoQF)	Game Theory, Vehicular edge computing (VEC) network	Compared to the rest of the consensus mechanisms studied, it has less loss when validating events but this has the impact of the longest delay in message transmission
[47] Sensing Accuracy	Permissioned Blockchain & Smart Contracts	Delegated Proof-of-Stake (DPoS)	Deep Neural networks (DNN)	Position correction compared to other methodologies is more effective when we have many errors from the sensors
[48] Audit	Blockchain	Proof-of-Storage	-	Moderate transmission speed performance – High security

5.2. Approaches for Social Challenges

The methodologies that face the above technical challenges are the basis for addressing more complex challenges that will make CCAM an acceptable solution for people's transportation in smart

 doi:10.20944/preprints202407.0493.v1

cities. The road safety that should be provided by autonomous vehicles for citizens to trust and use will be combined with in-vehicle infotainment systems thus helping the road system to be able to respond to green mobility and sustainable urban lifestyles. At the same time, the use of resources in financial terms is another challenge of VANET networks.

To save resources especially in storage space during the transmission and storage of the events in a road network with the aim of doing it efficiently and in a short time so as to avoid road accidents, the authors of [49] propose the combination of Transactions Filtering Pattern Matching Scheme (TFPMS) and blockchain technology to ensure data privacy and immutability. The architecture consists of 3 layers: Vehicular, Edge and Cloud. All transactions are filtered to reject the wrong ones and save storage space on the central servers located in the cloud. Once the data is filtered, it is stored in the blockchain and what is deemed important for future use is uploaded to the cloud.

Road safety applications in modern VANET networks are based on the periodic exchange of vehicle status (Basic Safety Messages, BSMs) via V2X communications over the new 5G New Radio (NR) specification, i.e., 5G NR V2X communications. The purpose of [50] is to improve the performance of New Radio V2X sidelinks (NR-V2X sidelink) over the existing Sensing-Based Semi-Persistent Scheduling (SPS) methodology. The proposed methodology reduces conflicts and improves communication performance by enhancing it by applying blockchain technology with a DPoS consensus mechanism. The vehicles are organized into platoons in which one vehicle is the Platoon Leader (PL) and is responsible for its control and the other vehicles are the Platoon Members (PM).

The authors of [51] propose a methodology in which electric vehicles (EV) will participate safely but also with the aim of reducing the consumption of electricity in the smart grid network of a smart city. To reduce the risk of Sybil Attacks and double spending and to prevent vehicles from operating selfishly when it comes to the use of the energy network, they apply blockchain technologies for attacks and smart contracts for “fairness” in consumption. Also, the use of smart contracts is used to protect customer vehicles and the public electricity network from incorrect and irregular charges.

In [52] a VANET payment system based on blockchain technology is proposed in which the blockchain network is maintained in RSUs and the vehicles generate the transaction content. In the proposed model vehicles relay on the lower level. On the higher lever there is the blockchain layer. Trading between one vehicle and one RSU is called V-R transaction while trading between one vehicle and multiple RSUs is called V-Rs transaction. These 2 types of transactions are respectively applied in the scenarios: park toll management system and electronic toll collection system (ETC). This particular methodology is a simple approach without considering how blocks are verified.

Electric cars’ range and ways to set up an effective charging infrastructure is the main subject of [53]. The lack of charging stations can be addressed by exchanging energy from neighboring vehicles that have available energy. for the design and implementation of this idea we should consider parameters such as the availability of charging stations, the length of time for charge, the cost, and the reliability of the service. The problem it this idea is the effective supplier selection along with the security and the uninterrupted exchange between buyer-seller. This methodology provides a mechanism for a novel VANET-based multi-criteria supplier selection based on the NDN framework and a blockchain technology to guarantee security and uninterrupted exchange. The basic features of the model is trust enforcement, Secure authentication of trading entities and supplier selection

To overcome problems of security, computational capabilities and especially scalability in the Social Internet of Vehicles (Social IoV) a methodology is proposed in [54] based on a two-dimensional blockchain and a dynamic consensus mechanism that implements the use of checkpoint-blocks for better use of vehicle resources and mobile points at the “edge” of the network. The architecture of the work consists of the vehicles, the RSUs which act as miners but also which are responsible for the registration of the vehicles, the Server/Miner which provides the blockchain network, the Edge Modules which are responsible for the protection from “overflow” of vehicle data but also for the management and allocation of resources. The consensus mechanism is dynamic (dynamic PoW, dPoW) which consists of 4 levels of difficulty which are applied depending on the rate of incoming traffic to SIoV data and which balance security with performance. The proposed methodology is

 doi:10.20944/preprints202407.0493.v1

evaluated according to the parameters: scalability, security, privacy and latency. A summary of the discussed approaches towards social challenges of CCAM, as well as their technical features are shown in Table 4 and Table 5 respectively.

Table 4. Blockchain and smart contract methodologies for social CCAM challenges.

Ref	Challenge	Summary	Advantages	Disadvantages
[49]	Road Safety	Improving the performance of communications in VANET road safety applications with the help of Blockchain technology	It reduces the need for processing power in vehicles	Stored feature policies are not dynamic and do not change.
[50]	Road Safety	Filtering event data and storing it on blockchain for road safety through false event protection	Efficient technique in a large and dense number of vehicles	-
[51]	Resource Management	Energy exchange methodology between charging stations and vehicles with the aim of saving energy and security from 2 types of attacks using blockchain & smart contracts.	Elimination of cheaters, complete supplier coverage with short time of searching and reduces costs for purchasers	There is no integration with IoV Infrastructure
[52]	Financial	Electronic payment methodology in VANETs based on blockchain	The communication load increases linearly in relation to the number of vehicles and not exponentially as it happens in pre-existing techniques.	Data transmission performance decreases for vehicles that are further away from other RSUs.
[53]	Financial	A methodology for supplier selection with secure buyer-seller exchange in Smart EV charging to mitigate anxiety in VANETs	Fast transaction transfer	The authentication mechanism and communications architecture are not described
[54]	Social Networking	Dynamic PoW mechanism based on checkpoint-block and different difficulty levels to manage IoV social network data	Low delays in V2I communications	Cloud servers pose a problem as far as the distributed feature of the methodology is concerned

 doi:10.20944/preprints202407.0493.v1

Table 5. Technical features of blockchain and smart contracts' methodologies for social CCAM challenges.

Ref Challenge	Blockchain / Smart Contract	Consensus mechanism	Techniques/tools	Performance of the methodology
[49] Road Safety	Blockchain	PoW	Distributed Cloud Servers	Low efficiency: Linear increase in both storage space and operating costs in line with the increase in vehicles
[50] Road Safety	Blockchain	Delegated Proof-of-Stake (DPoS)	5G New Radio (NR) V2X	High performance compared to the SPS technique in terms of collision probability and delay.
[51] Resource Management	Consortium Blockchain & Smart Contracts	Proof of Authority	Smart Grid	Moderate energy saving performance compared to existing solutions.
[52] Financial	Blockchain	PoW	-	High performance in relation to the time needed to search for a location but also the reduction of congestion and costs
[53] Financial	Blockchain	PoW	Named Data Networking, Vehicular Sensor Networks	Moderate performance relative to pre-existing works. Effectiveness: collection reporting, fake identical rate & time for trade
[54] Social Networking	Permissioned Blockchain	dynamic PoW (dPoW)	-	High: Compared to existing methodologies, this one performs better on a large increase in social network data and offloads vehicles from resource consumption

5.3. Approaches for Ethical Challenges

If the above challenges are addressed, they will offer a more mature and reliable automatic and autonomous driving, thus increasing the trust of citizens as well as the degree of penetration of autonomous vehicles in daily commuting. Safe driving and economy in time and cost as found in the previous section are key parameters for this penetration. According to the research of the first chapter the improvement of trust is an important ethical challenge for the CCAM. At the same time, the accountability of an accident should be based on parameters such that the result is not disputed. The person responsible for the accident should not be able to deny the incident he caused.

In this direction, the authors of the paper [55] propose a framework in which they combine blockchain and Named Data Networking (NDN) technologies with awareness of privacy and security in V2X communications and which they call Secure-V2X. This particular methodology does not use the private information of the parties involved (drivers, passengers, pedestrians, etc.) but non-private information such as the license plate number. An important addition to the methodology is that the maintenance and preservation of the blockchain network is not based on RSUs or other fixed infrastructures but on vehicles that are organized in clusters. To achieve consensus, multiple head vehicles participate in the process making the methodology suitable for protection against

 doi:10.20944/preprints202407.0493.v1

privacy attacks as well as DoS. The aim of the work is to assign responsibility to the vehicles without revealing their identity.

In order to maintain immutability but also make it possible to hold vehicles accountable when sharing the data, they collect through VANETs, the authors of the paper [56] propose combining blockchain technologies and smart contracts in parallel with the new features introduced by 5G communication networks and the media management of software-defined networks (SDNs) technology. Authorized users store the data in the blockchain network while large files such as video files are stored in the IPFS (InterPlanetary file system) file system. Those users who produce the message data are called owners while the rest of the users are the consumers and who search for the messages. There is also the trusted authority (TA) which is a trusted off-chain third party to create the system parameters, distribute keys and deploy smart contracts. The above model also involves the blockchain network to which both owners and consumer users have access. The network architecture is based on SDN technology to reduce delays in uploading and downloading data through 5G communications. The registration of messages by user-owners is based on keywords, which words are searched for by user-consumers by confirming them using smart contracts.

In the work of [57], it is presented a reputation evaluation model based on the logistic regression model by quantifying the behavior records of the distributed authentication entities. The methodology is a hierarchical certificate service chain based on reputation called HCSC, by introducing master authorities (MAs), certification authorities CAs, and roadside unit authorities (RSAs) in the blockchain network to monitor authentication entities (AEs) for providing reliable and transparent certifications. The suggested model is based on the blockchain architecture with 4 layers: data, network, consensus, and application and is efficient for the management of distributed authentication entities. Finally, the performance of certificate service is suitable for node authentication in VANETs.

The methodology of [58] is a combination of blockchain, SDN (Software-defined networking) and fog computing technologies to effectively manage and control the network in VANETs. The above technologies use 5G communication technology and fog computing technology to avoid frequent base changes (handovers) from vehicles, while the blockchain layer is included in the control plane of SDN. Also, the consensus mechanism practical Byzantine fault tolerance (PBFT) is used in order to ensure consistency between many involved entities in the model. RSUs act as miners, while the leader is elected from among themselves to create the blocks of the chain. There is a small group of default nodes that participate in the voting process to verify a block before reaching consensus. The methodology is based on immutable and distributed blockchain features to support the trust of messages, which are evaluated and scored by giving them a reputation score that is registered in the blockchain.

The authors of the work [59] analyze the importance of responsibility and fairness of VANET vehicles and propose a methodology based on the calculation of the reputation value of a node which is stored in a distributed network and while the remaining nodes searches through smart contract technology. Each vehicle not only has the right to investigate the reputation of a node, but also contributes to its evaluation process, having a clear view of what is happening in the evaluation process. The storage of the messages of the transmitted events is not done in a blockchain network but in the distributed Interplanetary file system (IPFS) network which costs less and has greater potential in storage space. Through smart contracts it is ensured that only the authorized party modifies the content, shares and updates the blockchain in the form of an IPFS hash of the hash ID. The above methodology provides decentralization, transparency, immutability to peer nodes, which leads to consistency of the reputation value of each user. A summary of the discussed approaches towards ethical challenges of CCAM, as well as their technical features are shown in Table 6 and Table 7 respectively.

The work of [60] concerns the design of a solution for trust management and for secure data transmission between vehicles and RSUs using the Physical Unclonable Function (PUF) performed by the embedded chips (System-on-chip – SoC) of vehicles along with blockchain technology. The use of PUFs gives each smart vehicle a unique cryptographic fingerprint (cID) which is used to

 doi:10.20944/preprints202407.0493.v1

determine the origin of the data. The network that supports the above solution is called DrivMan and for the communication and confirmation of the data transmission it uses 2 smart contracts, a public one between the network and the RSUs and a private one between the RSU and the vehicle. By using the above technologies and using a public key infrastructure (PKI), the authors propose the DrivMan methodology to facilitate trust management, data provenance and privacy. The authors assume that RSUs and the blockchain network do not have resource constraints, unlike the vehicle which does. Also, vehicles have SoCs with PUFs and any attempt to tamper with or remove PUFs will render communication useless.

Table 6. Blockchain and smart contract methodologies for ethical CCAM challenges.

Ref	Challenge	Summary	Advantages	Disadvantages
[55]	Accountability	Combining Blockchain and Named Data Networking (NDN) to provide secure distributed V2X communications while maintaining privacy.	The identity of the parties involved in the road network is not disclosed. It is an appropriate methodology to protect against identity disclosure and non-attribution attacks.	It has no filtering techniques for the data generated by the vehicle. Using different key pairs for blockchain and NDN functions puts a strain on system performance
[56]	Accountability	Event message search mechanism through blockchain and smart contracts maintaining the anonymity and accountability of VANET network users and improving the performance of the 5G network by applying SDN technology.	Reduces message transmission time and network load	It does not meet the needs of real-time VANETs.
[57]	Accountability	A hierarchical certificate service chain based on blockchain and on a new reputation measurement model for effective authentication of node's identity in VANETs	Small block storage pressure, and high consensus algorithm efficiency	Not tested in real scenarios
[58]	Responsibility	Propagation of messages based on reputation between connected vehicles and a combination of SDN, Fog Computing and blockchain technologies.	Platform capable of providing trust to the involved entities of VANETs	There are shortcomings in the methodology as far as privacy protection is concerned
[59]	Responsibility	A mechanism for generating, exchanging and storing the reputation of nodes in VANETs in order to encourage vehicle accountability.	The reputation score is available to individual nodes when requested with no central dependency.	The process of registering a vehicle does not guarantee concealment of the vehicle's location

 doi:10.20944/preprints202407.0493.v1

[60]	Trust management	Model for creating a distributed trust management system that registers and recalls vehicles using blockchain and smart contracts and the unique ID generated by the PUFs of the vehicles' SoCs.	It provides data with integrity, security and reliability.	Vulnerable to Modeling attacks on PUFs.

Table 7. Technical features of blockchain and smart contracts' methodologies for ethical CCAM challenges.

Ref	Challenge	Blockchain / Smart Contract	Consensus mechanism	Techniques/tools	Performance of the methodology
[55]	Accountability	Blockchain	PoW	Named data networking (NDN)	Moderate performance in the communication load due to the handling of a large amount of data by the vehicles but also due to the different key pairs used in the technologies based on
[56]	Accountability	Permissioned Blockchain & Smart Contracts	PoW	InterPlanetary File System (IPFS), Software-Defined Networks (SDNs)	Low performance
[57]	Accountability	Blockchain & Smart Contracts	Delegated proof of stake (DPoS), Proof of work (PoW)		Better for large concurrent authentication requests than a large number of requests
[58]	Responsibility	Blockchain	Practical Byzantine fault tolerance (PBFT)	SDN, Fog computing	Moderate performance in terms of communication load
[59]	Responsibility	Permissioned Blockchain & Smart Contracts	Proof of Authority	Interplanetary file system (IPFS)	Low performance as the number of malicious nodes increases, compared to the methodology without smart contracts
[60]	Trust management	Blockchain & Smart Contracts	PoW & Proof-of-Stake	Physical Unclonable Functions (PUFs)	Works effectively against data tampering and identity disclosure attacks

The primary purpose of all the previously presented methodologies is to deal with some attack or threat from malicious or untrusted nodes. According to [21] there are many and different types of attacks and threats, which must be addressed in order to make CCAM and CAVs suitable and reliable for daily safe use in transport. The types of attacks/threat that the blockchain and smart contract methodologies studied in this paper address, are shown in Table 8.

 doi:10.20944/preprints202407.0493.v1

Table 8. Blockchain and smart contract methodologies against threats/attacks.

Ref	Brute Force	Hijacking	Alteration Attack	Jamming	DDoS	Man-in-the-middle	51% Attack Resilience	Unlinkability	Intrusion Detection	Identity Authentication	User Account Management	Tracking Attack	Sybil Attack	Location Privacy Threats	Collusion Attack	Eavesdropping Attack
[42]	✓															
[43]							✓									
[44]		✓				✓	✓	✓								
[45]												✓				
[46]															✓	
[47]			✓									✓		✓		
[48]			✓	✓								✓				
[49]										✓						
[50]			✓												✓	
[51]													✓			
[52]											✓					
[53]							✓									
[54]		✓					✓									
[55]	✓				✓					✓						
[56]			✓													
[57]						✓							✓		✓	✓
[58]					✓											
[59]															✓	
[60]			✓					✓		✓						

6. Discussion and Future Directions

VANETs and especially CCAM, require high reliability and very low or zero delays. It is also particularly important to use computing and communication resources in a distributed and decentralized manner. For this purpose, blockchain technologies and smart contracts comprise an important application field of VANET networks. The analysis of the different methodologies described in the previous section reveals that the vast majority of studies addresses technical challenges and some of them go a step further and tackle higher level challenges such us social and ethical. Technical challenges include fundamental requirements such as data transmission security, privacy protection, accurate and reliable recording of events and messages, improved the data output by vehicle computing systems and sensors and distributed and decentralized operation of VANETs [15]. Social and ethical challenges have significant value and effect on daily lives of people who will use CCAM. Starting from addressing issues related to road safety, economy and environmental protection, we end up with issues of accountability and responsibility and finally of trust and safety [13].

What we can observe is that not all the methodologies examined in our study face CCAM challenges using a combination of blockchain and smart contracts. Specifically, about a third (35%) of them rely on smart contracts over blockchain mainly based on the Ethereum platform. There is

 doi:10.20944/preprints202407.0493.v1

also high variation in the implementation of consent mechanisms. Most of the works apply the classic mechanisms of Blockchain networks: Proof-of-Work, Proof-of-Stake, Delegated Proof-of-Stake, Proof- of-Authority and Practical Byzantine Fault Tolerance. However, several of them implement improved or enhanced mechanisms in terms of performance and communication load. Examples of these mechanisms are: Enhanced Delegated Proof-of-Stake, dynamic Proof-of-Work, Crash fault tolerance and Directed Acyclic Graph. However, in some works specialized or new mechanisms are applied which perform more effectively for the specific architecture of the methodology: Proof-of-Storage, Proof-of-Quality-Factor and Adaptive delegate consensus algorithm.

Due to the requirements in processing power, storage space and communication range, the functions of the Blockchain network and the corresponding consensus mechanisms, most methodologies apply the block mining process and the consensus mechanism either to the RSU nodes or to the servers located in central infrastructures or infrastructures at the edges of the network (edge servers) [21]. However, the use of RSUs and Edge Servers and in a few cases central infrastructure for mining and block creation, is not in the direction of decentralized and distributed VANET implementation, something which is a critical factor for the application of CCAM in the life of the citizens of a smart city. On the other hand, the important role of RSUs is mentioned in all the works since they are the means of communication and interconnection with the central network and the internet of vehicles.

Also, most of the proposed methodologies were evaluated through simulations. This raises concerns about the performance of the methodologies in real environments and in real-world implementations of the road ecosystem. At this point, it is worth mentioning the interesting three works in addressing the challenges in VANET networks in which unmanned aerial vehicles (UAVs) participate. UAVs are an emerging area of intelligent transportation systems with applications in both cargo transportation and monitoring and prevention.

Our literature review revealed various potential future directions for blockchain and smart contracts in CCAM, as summarized in Table 9. It is a requirement of CCAM users to create well-structured trust models to create an environment of trust and acceptance by smart city citizens towards smart road networks [20]. These models should be based on entities, on data exchanged and on context constraints considering different properties, metrics, and parameters. As described in chapter 5, many of the tasks address the various challenges with moderate or low performance and with low QoS indices. To increase the QoS indicators, common properties and characteristics should be defined on which future research and studies of VANETs and CCAMs will be based [61]. Examples of these properties or characteristics are reliable and accurate data transmission, communication cost, user privacy, and data security. On the other hand, once the common characteristics are defined and, in accordance with them, the new methodologies are applied, their results should be evaluated according to specific evaluation parameters. In other words, specific but also common evaluation parameters should be defined for all parties involved in the research process and study. Examples of the evaluation parameters could be the consumption and use of resources, the communication cost and range but also the different types of movement and vehicles, the environmental conditions, spatial parameters, etc.

Table 9. Potential future directions of CCAM.

Future direction	Description
Well-structured trust models	Models that will create a climate of trust and security for users and that will include all involved entities, different types of data, different properties, measurements and parameters.
Building a framework to protect against a set of attacks	Methodologies should cover many different types of attacks and not just a few. A comprehensive framework for dealing with most VANET attacks and failures should be designed and evaluated.

 doi:10.20944/preprints202407.0493.v1

Mechanisms and methodologies with a small energy footprint	Defining parameters in the processes and operations that will be implemented in order to reduce the consumption of resources that affect energy consumption and environmental pollution.
Comprehensive profiling, reputation and rating system for all entities involved	Creating a profile based on the contribution to road incident data, but also defining the reputation of each entity (fixed or not, direct or indirect), but also creating a reward system for its behavior in the road ecosystem.
Use of Federal Learning and Artificial Intelligence technologies.	Applying Federated Learning and Artificial Intelligence models to create a global intelligence in the IoT ecosystem.
Use of emerging technologies	Cloud Services, Fog & Edge computing, Software Defined Networking (SDN), Network Functions Virtualization (NFV).
Improving the performance of Blockchain technology for use in different applications	Blockchain offers users many different applications with different performance requirements, which must be met by Blockchain technology in order to overcome latency and load issues.
Improvement and development of detection systems and sensors	Further research into the creation of more reliable and efficient devices and sensors, filtering and evaluating the data they produce before being sent to the RSUs and central infrastructure.
Balancing between decentralization and network load	Blockchain technology, the consensus mechanism and the constant exchange of large volumes of data burdens the network and causes load and delays.
Allocation of resources, processing and storage	Due to the complexity and decentralization of Blockchain technology, as well as the dynamic nature of the blockchain, new performance and resource allocation challenges arise.

The characteristics of blockchain technology are a building block to protect against different kinds of attacks with the goal of securing communications, privacy and failure of systems that manage VANET networks. However, in each of the methodologies studied in the work, it was found that they do not cover a wide range of different types of attacks [43]. Perhaps the combination of several methodologies can provide protection against a set of attacks, proposing a framework that will fully protect VANETs and autonomous and connected vehicles from attacks. The resilience of CCAM to such attacks is critical for the safety of people and especially for services provided such as emergency transport in the event of accidents or disasters (ambulances, fire and police vehicles).

The applied methodologies should also consider environmental parameters primarily aiming to decrease the consumption of energy and resources [62]. The performance of the methodologies should be evaluated in the direction of reducing the load and delays in the various complex processes and calculations, thus creating frameworks with a small energy footprint and less burden on the environment. In this way, the CCAM will be a key structural component of smart and green mobility.

Moreover, various methodologies related to trust management, accountability, and road safety, which were based on the application of techniques and systems that evaluate, reward or not, users but also create the parameter of reputation in profile of the vehicle or the user [20]. These techniques rate a vehicle and create a reputation for that vehicle, based on its behavior in the road network and its contribution to traffic data sharing as well as to the transmission and confirmation of a road incident. However, each of the above methodologies examines different entities that participate in the road ecosystem: some concern the behavior of driver-passengers, others the behavior of vehicles and others the reliability of fixed nodes such as RSUs. Therefore, to improve reliability and trust, systems should be designed that involve all the entities: fixed and mobile hubs, drivers and passengers, but also pedestrians or users of bicycles, skates and public transport. These systems will

 doi:10.20944/preprints202407.0493.v1

include the creation of an overall profile which will have as parameters: the reputation of each entity, the degree of contribution and the overall score in the road ecosystem of the smart city.

An important technology in VANET networks is AI, which is already applied to some of the methodologies we reviewed, with the aim of better data transmission, their evaluation and decision-making. Optimizing these models towards creating a global intelligence of the entire IoV ecosystem with distributed and decentralized features is a major challenge of the methodologies. To complete this optimization and make the CCAM trustworthy and reliable, Federated Learning (FL) needs to be implemented alongside AI [63]. Collaborative learning by collecting knowledge from different devices or entities will improve the overall intelligence of the system thus having a significant impact on building trust between human and autonomous vehicle as well as the road safety of CCAM. Nevertheless, the combination of blockchain technology with FL and AI in environments without centralized management but in a distributed network of cooperative intelligence is the subject of further study and investigation.

Along with the previous technologies, other emerging technologies should be implemented, such as fog and edge computing, Software Defined Networking (SDN) and Network Functions Virtualization (NFV) [64,65]. Their implementation should be based on future research and methodologies combined with Blockchain and IoV technologies to extend the original VANET networks to V2X communications. The above technologies will help to provide better QoS indicators and architectures that will ensure dynamic, reliable and secure trust management as well as performance of responsibilities to the parties involved in smart mobility while at the same time using Blockchain, data will remain immutable, durable and traceable. Cloud, SDN and NFV technologies create conditions of dynamism, scalability, better network management and resource sharing [66]. However, architectures and methodologies based on cloud and SDN services need further investigation due to both the delay of data transmission between nodes and infrastructures, as well as security and privacy issues that arise.

In many of the methodologies we studied, performance issues of the functions required by blockchain and Smart contract technologies were observed, especially during the creation of the blocks and during the execution of consensus mechanisms. The performance issues concerned both the delay of the above processes, the energy consumption, and the communication load they create. Autonomous and interconnected vehicles are the most important part of CCAM. The latter provides citizens with many IoT and IoV applications based on blockchain technology. Each of these applications has different characteristics and requirements: a road emergency system has different delay requirement from a parking space management system. Another example is the vehicle's collision avoidance mechanism, which requires zero delays and reliable, error-free data transmission [67]. Therefore, studies and research should also focus on the design of more efficient frameworks utilizing blockchain for heterogeneous applications.

The overall performance of the network due to the exchange of a large amount of data before the blockchain consensus is reached, is affected by the large network load of maintaining the blockchain network. The decentralized nature of the latter and the consensus mechanism results in an increase in network load and delays, which causes a significant problem especially in cases where the range of communications is limited. So, the above should be considered when implementing blockchain in VANETs as it is necessary to consider the balance between decentralization and network load.

7. Conclusions

This study presented the basic challenges of cooperative, connected and automated mobility grouping them in three categories: technical, social and ethical. Contrary to previous related surveys, we explore solutions for addressing all three categories of challenges in vehicular networks. First, we identified and described twelve (12) major challenges and then we analyzed the most contemporary methodologies and techniques that use blockchain and smart contracts to deal with each challenge. Additionally, we took a deep dive into the main characteristics, advantages, and disadvantages of each methodology providing a comparative analysis and we identified different types of attacks and

threats they deal with. We critically discussed our finding and attempt to delineate the future directions of CCAM taking under consideration how these interact with blockchain. What can lie concluded is that there is still a long way to go before blockchain can be used efficiently in CCAM to overcome latency and load issues especially for the consensus mechanism.

Author Contributions: Conceptualization, C.K.; methodology, C.K. and T.P.; investigation, C.K.; writing—original draft preparation, C.K.; writing—review and editing, C.K and T.P.; visualization, C.K. and T.P.; supervision, A.K.; project administration, A.K.; funding acquisition, A.K. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the Erasmus+ project "OpenDCO - Open Data City Officer", grant number 22022-1-CY01-KA220-HED-000089196.

Data Availability Statement: No new data were created or analyzed in this study. Data sharing is not applicable to this article.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Faria, R.; Brito, L; Baras, K.; Silva, J. Smart mobility: A survey. In Proceedings of the IEEE International Conference on Internet of Things for the Global Community, Funchal, Portugal, 10-13 July 2017
2. Mukhtar-Landgren, D.; Paulsson, A. Governing smart mobility: policy instrumentation, technological utopianism, and the administrative quest for knowledge. *Adm. Theory Prax.* **2021**, 43, 135-153
3. Papa, R.; Gargiulo, C.; Russo, L. The evolution of smart mobility strategies and behaviors to build the smart city. In Proceedings of the 5th IEEE International Conference on Models and Technologies for Intelligent Transportation Systems, Napoli, Italy, 26-28 June 2017
4. Piperigkos, N.; Anagnostopoulos, C.; Lalos, A. S.; Berberidis, K. Extending Online 4D Situational Awareness in Connected and Automated Vehicles. *IEEE Trans. Intell. Veh.* **2023**, 1-19
5. Oladimeji, D.; Gupta, K.; Kose, N. A.; Gundogan, K.; Ge, L.; Liang, F. Smart transportation: an overview of technologies and applications. *Sensors* **2023**, 23, 3880
6. Rai, S. C.; Nayak, S. P.; Acharya, B.; Gerogiannis, V. C.; Kanavos, A.; Panagiotakopoulos, T. ITSS: An Intelligent Traffic Signaling System Based on an IoT Infrastructure. *Electronics* **2023**, 12, 1177.
7. Wang, Y.; Cai, P.; Lu, G. Cooperative autonomous traffic organization method for connected automated vehicles in multi-intersection road networks. *Transp. Res. C: Emerg. Technol.* **2020**, 111, 458-476.
8. Alonso Raposo, M.; Grosso, M.; Després, J.; Fernández Macías, E.; Galassi, C.; Krasenbrink, A.; ... Ciuffo, B. An analysis of possible socio-economic effects of a Cooperative, Connected and Automated Mobility (CCAM) in Europe. Available online: https://core.ac.uk/download/pdf/157830385.pdf (accessed on 30 June 2024)
9. Hang, P.; Lv, C.; Huang, C.; Xing, Y.; Hu, Z. Cooperative decision making of connected automated vehicles at multi-lane merging zone: A coalitional game approach. *IEEE Trans. Intell. Transp. Syst.* **2021**, 23, 3829-3841.
10. Rahman, M. H.; Abdel-Aty, M.; Wu, Y. A multi-vehicle communication system to assess the safety and mobility of connected and automated vehicles. *Transp. Res. C: Emerg. Technol.* **2021**, 124, 102887.
11. Piperigkos, N.; Lalos, A. S.; Berberidis, K. Multi-modal cooperative awareness of connected and automated vehicles in smart cities. In Proceedings of the 2021 IEEE International Conference on Smart Internet of Things (SmartIoT), Jeju, Korea, 13-15 August 2021
12. He, J.; Tang, Z.; Fu, X.; Leng, S.; Wu, F.; Huang, K.; ... Xiong, Z. Cooperative connected autonomous vehicles (CAV): research, applications and challenges. In Proceedings of the 27th IEEE International Conference on Network Protocols, Chicago, Illinois, USA, 7-10 October 2019
13. Peng, C.; Wu, C.; Gao, L; Zhang, J.; Alvin Yau, K. L.; Ji, Y. Blockchain for vehicular internet of things: Recent advances and open issues. *Sensors* **2020**, 20, 5079.
14. Zhu, X.; Gu, Z.; Wang, Z. Ethical Challenges and Countermeasures of Autonomous Vehicles. In Proceedings of the 2nd International Academic Exchange Conference on Science and Technology Innovation E3S Web of Conferences, Guangzhou, China, 18-20 December 2020.
15. Gruyer, D.; Orfila, O.; Glaser, S.; Hedhli, A.; Hautière, N.; Rakotonirainy, A. Are connected and automated vehicles the silver bullet for future transportation challenges? Benefits and weaknesses on safety, consumption, and traffic congestion. *Front. Sustain. Cities* **2021**, 63, 607054
16. Alladi, T.; Chamola, V.; Sahu, N.; Venkatesh, V.; Goyal, A.; Guizani, M. A comprehensive survey on the applications of blockchain for securing vehicular networks. *IEEE Commun. Surv. Tutor.* **2022**, 24, 1212-1239

17. Bonnefon, J. F.; Černy, D.; Danaher, J.; Devillier, N.; Johansson, V.; Kovacikova, T.; ... Zawieska, K. Ethics of Connected and Automated Vehicles: Recommendations on road safety, privacy, fairness, explainability and responsibility. European Commission **2020**
18. Cunneen, M.; Mullins, M.; Murphy, F.; Shannon, D.; Furxhi, I.; Ryan, C. Autonomous vehicles and avoiding the trolley (dilemma): vehicle perception, classification, and the challenges of framing decision ethics. *Cybern. Syst.* **2020**, 51, 59-80.
19. Martinho, A.; Herber, N.; Kroesen, M.; Chorus, C. Ethical issues in focus by the autonomous vehicles industry. Transp. Rev. **2021**, 31, 556-577.
20. Hbaieb, A.; Ayed, S.; Chaari, L. A survey of trust management in the Internet of Vehicles. *Comput. Netw.* **2022**, 203, 108558.
21. Zekri, A.; Jia, W. Heterogeneous vehicular communications: A comprehensive study. Ad Hoc *Netw.* **2018**, 75, 52-79.
22. Wei, S.; Zou, Y.; Zhang, X.; Zhang, T.; Li, X. An integrated longitudinal and lateral vehicle following control system with radar and vehicle-to-vehicle communication. *IEEE Trans. Veh. Technol.* **2019**, 68, 1116-1127.
23. Lee, M.; Atkison, T. VANET applications: Past, present, and future. *Veh. Commun.* **2021**, 28, 100310
24. Al-Heety, O. S.; Zakaria, Z.; Ismail, M.; Shakir, M. M.; Alani, S.; Alsariera, H. A comprehensive survey: Benefits, services, recent works, challenges, security, and use cases for sdn-vanet. *IEEE Access* **2020**, 8, 91028-91047.
25. Shan, M.; Narula, K.; Wong, Y. F.; Worrall, S.; Khan, M.; Alexander, P.; Nebot, E. Demonstrations of cooperative perception: Safety and robustness in connected and automated vehicle operations. *Sensors* **2020**, 21, 200.
26. Mahi, M. J. N.; Chaki, S.; Ahmed, S.; Biswas, M.; Kaiser, M. S.; Islam, M. S.; ... Whaiduzzaman, M. A review on VANET research: Perspective of recent emerging technologies. *IEEE Access* **2022**, 10, 65760-65783
27. Son, S.; Lee, J.; Park, Y.; Park, Y.; Das, A. K. Design of blockchain-based lightweight V2I handover authentication protocol for VANET. *IEEE Trans. Netw. Sci. Eng.* **2022**, 9, 1346-1358
28. Nakamoto, S. Bitcoin: A peer-to-peer electronic cash system. *Dec. Bus. Rev.* **2008**, 21260
29. Antonopooulos, A. M. Mastering Bitcoin: unlocking digital cryptocurrencies; O'Reilly Media, Inc, 2014
30. Cebe, M.; Erdin, E.; Akkaya, K.; Aksu, H.; Uluagac, S. Block4forensic: An integrated lightweight blockchain framework for forensics applications of connected vehicles. *IEEE Commun. Mag.* **2018**, 56, 50-57
31. Rathee, G.; Sharma, A.; Iqbal, R.; Aloqaily, M.; Jaglan, N.; Kumar, R. A blockchain framework for securing connected and autonomous vehicles. Sensors **2019**, 19, 3165
32. Fu, Y.; Yu, F. R.; Li, C.; Luan, T. H.; Zhang, Y. Vehicular blockchain-based collective learning for connected and autonomous vehicles. IEEE wireless communications **2020**, 27, 197-203
33. Mik, E. Smart contracts: terminology, technical limitations and real world complexity. *Law Innov. Technol.* **2017**, 9, 269-300.
34. Khan, S. N.; Loukil, F.; Ghedira-Guegan, C.; Benkhelifa, E.; Bani-Hani, A. Blockchain smart contracts: Applications, challenges, and future trends. *Peer-to-Peer Netw. Appl.* **2021**, 14, 2901-2925
35. Christidis, K.; Devetsikiotis, M. Blockchains and smart contracts for the internet of things. *IEEE Access* **2016**, 4, 2292-2303
36. Hasan, H. R.; Salah, K. Proof of delivery of digital assets using blockchain and smart contracts. *IEEE Access* **2018**, 6, 65439-65448
37. Waltl, B.; Sillaber, C.; Gallersdörfer, U.; Matthes, F. Blockchains and smart contracts: a threat for the legal industry?. In *Business Transformation through Blockchain*, Volume II; Treiblmaier, H., Beck, R., Eds.; Springer Nature: Cham, Switzerland, 2019; 287-315.
38. Aoun, A.; Ilinca, A.; Ghandour, M.; Ibrahim, H. A review of Industry 4.0 characteristics and challenges, with potential improvements using blockchain technology. *Comput. Ind. Eng.* **2021**, 162, 107746
39. Zheng, Z.; Xie, S.; Dai, H. N.; Chen, W.; Chen, X.; Weng, J.; Imran, M. An overview on smart contracts: Challenges, advances and platforms. *Future Gener. Comput. Syst.* **2020**, 105, 475-491.
40. Kitchenham, B.; Pretorius, R.; Budgen, D.; Brereton, O.P.; Turner, M.; Niazi, M.; Linkman, S. Systematic Literature Reviews in Software Engineering—A Tertiary Study. *Inf. Softw. Technol.* **2010**, 52, 792–805
41. Moher, D.; Liberati, A.; Tetzlaff, J.; Altman, D. G.; Prisma Group. Preferred reporting items for systematic reviews and meta-analyses: the PRISMA statement. *Int. J. Surg.* **2010**, 8, 336-341
42. Zhang, X.; Chen, X. Data Security Sharing and Storage Based on a Consortium Blockchain in a Vehicular Ad-hoc Network. *IEEE Access* **2019**, 7, 58241-58254
43. Shrestha R.; Nam, S. Y. Regional Blockchain for Vehicular Networks to Prevent 51% Attacks. *IEEE Access* **2019**, 7, 95033-95045
44. Lin, C.; He, D.; Huang, X.; Kumar, N.; Choo, K. K. R. BCPPA: A blockchain-based conditional privacy-preserving authentication protocol for vehicular ad hoc networks. *IEEE Trans. Intell. Transp. Syst.* **2020**, 22, 7408-7420.
45. Zheng, D.; Jing, C.; Guo, R.; Gao, S.; Wang, L. A traceable blockchain-based access authentication system with privacy preservation in VANETs. *IEEE Access* **2019**, 7, 117716-117726.

46. Ayaz, F.; Sheng, Z.; Tian, D.; Guan, Y. L. A proof-of-quality-factor (PoQF)-based blockchain and edge computing for vehicular message dissemination. *IEEE Internet Things J.* **2020**, 8, 2468-2482.
47. Li, C.; Fu, Y.; Yu, F. R.; Luan, T. H.; Zhang, Y. Vehicle position correction: A vehicular blockchain networks-based GPS error sharing framework. *IEEE Trans. Intell. Transp. Syst.* **2022**, 22, 898-912.
48. Ma, J.; Li, T.; Cui, J.; Ying, Z.; Cheng, J. Attribute-Based Secure Announcement Sharing Among Vehicles Using Blockchain. *IEEE Internet Things J.* **2021**, 8, 10873-10883
49. Iftikhar, M. Z.; Javaid, N.; Javaid, S.; Imran, M.; Nasser, N. TFPMS: Transactions Filtering Pattern Matching Scheme for Vehicular Networks based on Blockchain. In Proceedings of the 2020 International Wireless Communications and Mobile Computing (IWCMC), online, 12-14 October 2020
50. Cao, L.; Yin, H. A Blockchain-Empowered Platoon Communication Scheme for Vehicular Safety Applications. In Proceedings of the 2021 IEEE 94th Vehicular Technology Conference, online, 27 September – 28 October 2021.
51. Khalid, R.; Malik, M. W.; Alghamdi, T. A.; Javaid, N. A consortium blockchain based energy trading scheme for Electric Vehicles in smart cities. *J. Inf. Secur. Appl.* **2021**, 63, 102998
52. Deng, X.; Gao, T. Electronic payment schemes based on blockchain in VANETs. *IEEE Access* **2020**, 8, 38296-38303
53. Vendan, V.; Chaudhary, A. Smart EV Charging to Mitigate Range Anxiety in VANET Backbone Guided by Named Data Networking and Block-Chain. In Proceedings of the 2023 International Conference on Distributed Computing and Electrical Circuits and Electronics (ICDCECE), Ballar, India, 29-30 April 2023
54. Javaid, U.; Sikdar, B. A Secure and Scalable Framework for Blockchain Based Edge Computation Offloading in Social Internet of Vehicles. *IEEE Trans. Veh. Technol.* **2021**, 70, 4022-4036.
55. Rawat, D. B.; Doku, R.; Adebayo, A.; Bajracharya, C.; Kamhoua, C. Blockchain Enabled Named Data Networking for Secure Vehicle-to-Everything Communications. IEEE Netw. **2020**, 34, 185-189
56. Yeh, L. Y.; Shen, N. X.; Hwang, R. H. Blockchain-based privacy-preserving and sustainable data query service over 5G-VANETs. *IEEE Trans. Intell. Transp. Syst*. **2022**, 23, 15909-15921.
57. Zhu, Q.; Jing, A.; Gan, C.; Guan, X.; Qin, Y. HCSC: A Hierarchical Certificate Service Chain Based on Reputation for VANETs. *IEEE Trans. Intell. Transp. Syst* **2023**, 24, 6123-6145
58. Gao, J.; Agyekum, K. O.-B.; Sifah, E. B.; Acheampon, K. N. A Blockchain-SDN-Enabled Internet of Vehicles Environment for Fog Computing and 5G Networks. *Internet Things J.* **2020**, 7, 4278-4291
59. Malik, N.; Nanda, P.;, He, X.; Liu, R. Trust and Reputation in Vehicular Networks: A Smart Contract-Based Approach. 2019 In Proceedings of the 18th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/13th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE), Rotorua, New Zealand, 5-8 August 2019
60. Javaid, U.; Aman, M. N.; Sikdar, B. DrivMan: Driving trust management and data sharing in VANETS with blockchain and smart contracts. In Proceedings of the IEEE 89th Vehicular Technology Conference, Kuala Lumpur, Malaysia, 28 April - 1 May 2019
61. Kong, M.; Zhao, J.; Sun, X.; Nie, Y. Secure and efficient computing resource management in blockchain-based vehicular fog computing. China Commun. **2021**, 18, 115-125.
62. Bıyık, C.; Abareshi, A.; Paz, A.; Ruiz, R. A.; Battarra, R.; Rogers, C. D.; Lizarraga, C. Smart Mobility Adoption: A Review of the Literature. *J. Open Innov.: Technol. Mark. Complex.* **2021**, 7, 146
63. Gkillas, A.; Lalos, A. S.; Markakis, E. K.; Politis, I. A Federated Deep Unrolling Method for Lidar Super-resolution: Benefits in SLAM. IEEE Trans. Intell. Veh. **2023**
64. Sodhro, A. H.; Rodrigues, J. J.; Pirbhulal, S.; Zahid, N.; de Macedo, A. R. L.; de Albuquerque, V. H. C. Link optimization in software defined IoV driven autonomous transportation system. *IEEE Trans. Intell. Transp. Syst.* **2020**, 22, 3511-3520.
65. Wu, Y.; Dai, H. N.; Wang, H.; Xiong, Z.; Guo, S. A survey of intelligent network slicing management for industrial IoT: Integrated approaches for smart transportation, smart energy, and smart factory. *IEEE Commun. Surv. Tutor.* **2022**, 24, 1175-1211.
66. Ray, P. P.; Kumar, N. SDN/NFV architectures for edge-cloud oriented IoT: A systematic review. *Comput. Commun.* **2022**, 169, 129-153.
67. Gkillas, A.; Lalos, A. S.; Ampeliotis, D. An efficient deep unrolling super-resolution network for Lidar automotive scenes. In Proceedings of the 2023 IEEE International Conference on Image Processing (ICIP), Kuala Lumpur, Malaysia, 8-11 October 2023