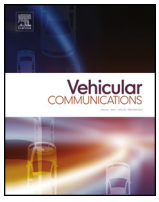
Vehicular Communications 43 (2023) 100607

Contents lists available at ScienceDirect

Vehicular Communications

journal homepage: www.elsevier.com/locate/vehcom



A comprehensive survey on blockchain-based C-ITS applications: Classification, challenges, and open issues

Souad BelMannoubi [b], Haifa Touati [a,*], Mohamed Hadded [c], Khalifa Toumi [d], Oyunchimeg Shagdar [e], Farouk Kamoun [b]

[a] Laboratoire Hatem Bettahar IResCoMath, Université de Gabès, Tunisia
[b] Laboratoire CRISTAL, Ecole Nationale des Sciences de l'Informatique, Université de la Manouba, Tunisia
[c] Abu Dhabi University, Abu Dhabi, United Arab Emirates
[d] IRT SystemX, Paris-Saclay, 91127 Palaiseau, France
[e] Institut VEDECOM, 23 bis Allée des Marronniers, Versailles, France

ARTICLE INFO

Article history:
Received 29 November 2021
Received in revised form 4 February 2023
Accepted 5 April 2023
Available online 8 May 2023

Keywords:
C-ITS
Vehicular networks
Blockchain
Consensus
Smart contract
Security
Privacy
Trust
Data sharing

ABSTRACT

Cooperative Intelligent Transport Systems (C-ITS) aim to improve road safety and provide comfort to both drivers and passengers by enabling vehicles, infrastructure, and other road users to exchange environmental and driving data. Therefore, the accuracy of the information exchanged as well as the authenticity of the entities, effectively affect the efficiency and performance of the system. Blockchain is a new distributed ledger technology that enables secure and transparent information storage and transmission without the control of a central entity. Its inherent features of trust, anonymity, immutability, and data availability offer great potential to solve current C-ITS issues. Recently, several research works are carried out to explore the potential of the blockchain technology in a vehicular environment. In this paper, we present a comprehensive review of the literature related to the application of the blockchain technology in C-ITS. We provide background knowledge on blockchain and the motivations for applying this technology in vehicular networks. Then, we discuss the major challenges that can bring the application of blockchains in a vehicular environment, such as mobility, latency, etc. Next, we review current research and classify it into four main categories. Moreover, a qualitative comparison of the discussed solutions is presented to identify the strengths and the weaknesses of each proposal. Finally, we highlight some open research issues that should be considered in future studies to improve the performance of blockchain-based vehicular systems.

1. Introduction

In the past few years, owing to the adoption of intelligent systems, the transport domain has experienced a particular development. Indeed, existing transport systems are being replaced with Intelligent Transport Systems (ITS) [1], [2], [3]. The emerging technologies of ITS contribute to solve the most important transport issues, namely traffic jams, and crashes. Nevertheless, such systems need to have the capability to interact, e.g., by enabling inter-vehicle cooperation [4]. For years, this interaction is enabled by two key access technologies, namely Dedicated Short-Range Communications (DSRCs) and cellular communications. Moreover, recent advances in access technology, such as the emergence of the sixth generation (6G) communications technologies, are expected to accommodate the extreme traffic demands of future ITS applications [5]. By improving throughput, reliability, and latency, emerging 6G technologies will be key factors to support the cooperation between already connected vehicles and with the entities on the road [6][7]. This interactivity is the area of C-ITS, which will enable road users to exchange data and use it to coordinate their activities. This cooperation, is achieved by the digital interconnectivity between different vehicles and road infrastructures. It aims to enhance traffic performance, and road safety and to assist the user in decision-making and adaptation to the road situation.
In C-ITS, vehicles cooperate by exchanging Vehicle-to-Everything (V2X) communication messages over vehicular networks. Road safety applications use data from these messages to effectively steer or monitor vehicles in order to avoid accidents and/or traffic jams, thus making driving safe and comfortable for drivers and passengers. Besides, information about events, such as accidents, is

* Corresponding author.
E-mail address: haifa.touati@univgb.tn (H. Touati).

https://doi.org/10.1016/j.vehcom.2023.100607
2214-2096/

vital and can be presented in legal proceedings as digital evidence. Therefore, it is crucial that the V2X message data be secure and accurate. Nevertheless, due to confidentiality and management concerns, realizing meaningful cooperation between entities owned by different parties remains a challenge. Moreover, to store and share all the information exchanged in the vehicular network, we need a secure, transparent, and immutable platform [8].

BlockChain (BC) technology [9], [10] is a novel distributed architecture that employs a special structural model to store and audit data. Consensus algorithms are used to create and append new data blocks. In addition, this new technology ensures system security by applying certain cryptographic techniques and by using smart contracts that allow automated data handling and access control. Strictly speaking, the blockchain is a cryptographically secured, tamper-proof and unfalsifiable distributed ledger that seamlessly links data blocks in chronological order.

When blockchain technology is implemented in vehicular networks as illustrated in Fig. 1, it offers several potential benefits, including greater decentralization, higher trust, better immutability, easier pseudonymity, more transparency, and enhanced automation. Blockchain is a system that is based on the complete decentralization of data recording and management. Indeed, instead of relying on a central entity that registers and controls the network, consensus algorithms are launched among the decentralized nodes to ensure consistency between the different stakeholders. Moreover, in a blockchain system, there is no need for a trusted third party, it can function entirely in peer-to-peer mode. In addition, blockchain can make data immutable, which can be considered as digital evidence. Accordingly, blockchain technology has the potential to strengthen the reliability of the entire system [13], by facilitating the interaction and communication among the entities [12], and by enhancing network data sharing [11]. Furthermore, the exchange of transactions in the blockchain network is based on the use of pseudonymous public addresses. Therefore, the real identities of users are kept hidden. Another feature of blockchain technology is transparency. All nodes in the system have access to the data stored in the blockchain ledger. Thus, each entity can verify the validity of the exchanged transactions. Finally, by integrating smart contracts with blockchain, certain operations can be automated, namely data storage and transaction generation.

Recently, industry and academia have paid considerable attention to emerging blockchain technologies [14]. The intrinsic characteristics of blockchain mentioned above, make it a potentially interesting tool to enhance the transport system and facilitate the processes between different companies in the automotive industry including car manufacturers, insurers, vehicle owners, etc. Furthermore, blockchain and smart contracts could help administer customs clearances, approvals, and document coordination in a more efficient, transparent, and secure manner and improve the accuracy of shared data [15]. For these reasons, leaders in the automotive industry such as Toyota, Porsche, Renault, Ford, and BMW are turning to blockchain to make vehicles autonomous and to improve the performance of their supply chains.

Several automotive blockchain use cases are rapidly shifting the market. Porsche has paired with the blockchain startup XAIN to implement blockchain technology in their vehicles [16]. The blockchain would allow users to unlock their vehicles with an application and to provide easier automated payment systems. In another example, Toyota Research Institute is partnering with MIT MediaLab and four other companies [17] to study how blockchain technologies can be useful for the automotive industry. One of the projects of this new consortium consists in facilitating the sharing of driving data. Furthermore, Renault has partnered with Microsoft to develop a blockchain-based data storage system [18]. Currently, Renault customers' details are housed in multiple databases, making it extremely difficult for the company to access this information quickly. The automaker turned to Microsoft to assist in the development of its own blockchain system to accelerate this process.

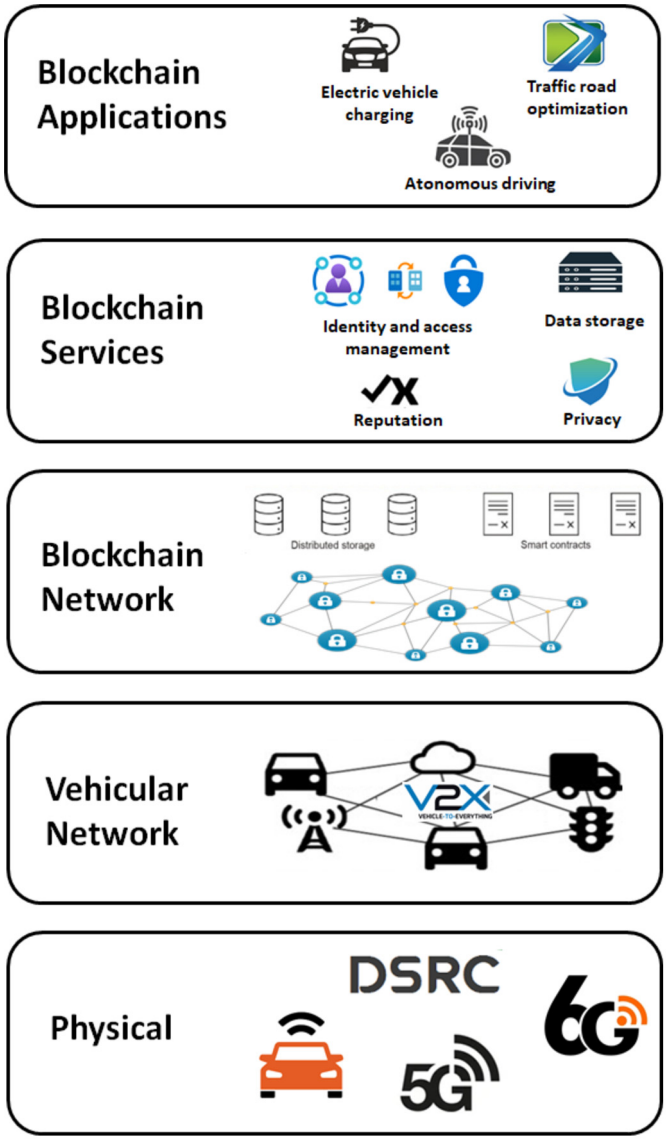


Fig. 1. Vehicular Network architecture after blockchain implementation.

Therefore, the automotive industry can immensely gain from the introduction of the blockchain, as this technology seeks to strengthen the automotive supply chain, vehicle safety and security, and car maintenance.

1.1. Related surveys

Blockchain is becoming a trendy technology that is being applied in different application areas. One of the major areas related to the application of this technology is the Internet of Things (IoT). We summarize some of the published literature studies regarding the integration of blockchain technology with IoT in Table 1. In [10], Xie et al. provided a comprehensive literature survey about the application of blockchain technology in smart cities. Similarly, in [19], Bhushan et al. addressed the security challenges of a smart city that uses blockchain technology. In another work [20], Ferrag et al. conducted a study to classify the existing threat models in IoT networks based on blockchain technology. However, the authors did not provide a detailed analysis of the context of ve-

Table 1
Summary and comparison of prior survey papers related to blockchain technology integration.

Reference	Year	objective	Merits	Demerits
[10]	2019	Outline a detailed review of research literature related to the integration of blockchain technology with smart cities	Discuss in detail and in depth research issues that will be addressed in the future	
[19]	2020	To survey solutions that propose to use the blockchain technology to overcome several security issues in smart cities applications	Study profoundly how blockchain can address certain smart cities issues namely security and privacy	Does not focus exclusively on vehicular networks
[20]	2019	Provide overviews on how the blockchain technology has been applied with IoT	To provide a taxonomy comparison of different solutions that address IoT security and privacy issues using blockchain	Does not focus exclusively on vehicular networks
[22]	2019	To present and analyze some example of VANETs applications based on blockchain technology	Discuss how VANETs can be protected and preserved from being alerted using blockchain	Only surveys papers based on VANETs applications and published between 2016 - 2018
[21]	2020	To survey and compare present VANET applications based on blockchain technology	Identify and analyze certa in challenges facing blockchain-based VANET systems	Focuses only on VANET solutions. They discuss papers that concentrate only on vehicles and RSUs as entities in the vehicular ecosystem
[23]	2020	Present a current investigation of the newest developments in the blockchain-based internet of vehicles systems	Highlight a number of new paradigm that can be used with blockchain-based vehicular applications, namely, edge computing, etc.	Does not focus on certain blockchain-based VANET applications challenges as mobility, latency, etc.
Our work	2021	We present a comprehensive survey that studies the impacts of the incorporation of blockchain technology into CITS. Our paper allows researchers to understand the advantages and the challenges associated with this integration	A qualitative comparison of the discussed solutions is presented according to different criteria. That aim to outline proposals' benefits and drawbacks in order to figure out the main issues in each architecture related to the integration of the blockchain.	

hicular networks. The authors of [21] introduced a survey that compares some of the existing proposals based on blockchain technology for Vehicular AdHoc Networks (VANET). They classified the blockchain-based VANET applications into four categories: security, trust establishment, incentive, and privacy preservation. Similarly in [22], some examples of blockchain applications in VANETs are presented and analyzed. More precisely, this paper surveys recent works related to the application of blockchain technology to secure autonomous vehicle communications. However, these two papers concentrate on solutions that used only Road-Side Unit (RSU) and vehicles as blockchain participants. Nevertheless, C-ITS is composed of other components than the above entities, such as applications and servers in the cloud and at the edge, vulnerable road users, drivers, riders, law enforcement authorities, etc. In [23] the authors focused on blockchain-enabled intelligent transport systems in general. They surveyed the recent advancements in blockchain-empowered applications, including edge computing and artificial intelligence. Further, they discussed the challenges and opportunities of blockchain-based applications in C-ITS. The above articles could be practical to understand the benefits of employing the blockchain in automotive networks by explaining the usefulness of the technology in C-ITS. However, they do not explain how the blockchain could be leveraged in the vehicular environment and what could be the main issues of each solution.

1.2. Contributions of this survey

Compared to prior studies on the implementation of blockchain technology in vehicular networks, in this review, we present a comprehensive and state-of-the-art study on the application of this technology in C-ITS.
The main contributions of this study include the following:

- We identify the most significant issues associated with the application of blockchain in vehicular environments. Particularly, we assess the impact of vehicles mobility on the blockchain operation, the influence of the blockchain latency problem on real-time C-ITS applications, the problem associated with storing the blockchain ledger on a limited storage space such as that of vehicles and RSUs, as well as communication overhead and security issues.
- We define a new classification of blockchain applications in vehicular networks. We identify four categories, namely, Identity and Access Management (IAM), reputation, privacy preservation, and data sharing. A summary is given at the end of each category to clarify the usefulness of the blockchain for each of them. Our classification could help both academics and industries to improve their understanding of this emerging research area.
- We present a qualitative comparison of the discussed solutions according to different criteria. The aim of this comparison is to identify the strengths and the weaknesses of each proposal and to figure out the main issues in each architecture that proposes to integrate blockchain technology in vehicular networks. This comparison helps researchers to develop more efficient blockchain-based vehicular systems.
- We highlight open research issues in blockchain technologies for C-ITS to guide scientists and practitioners, and show them where they should focus their future research.

1.3. Organization and reading map

We structure the rest of the paper as follows:
Section 2 provides an overview of blockchain technology, in particular, the main operation of a blockchain and its different types, the principle of consensus protocols, and the concept of smart contracts. Section 3 outlines the underlying motivation for introducing

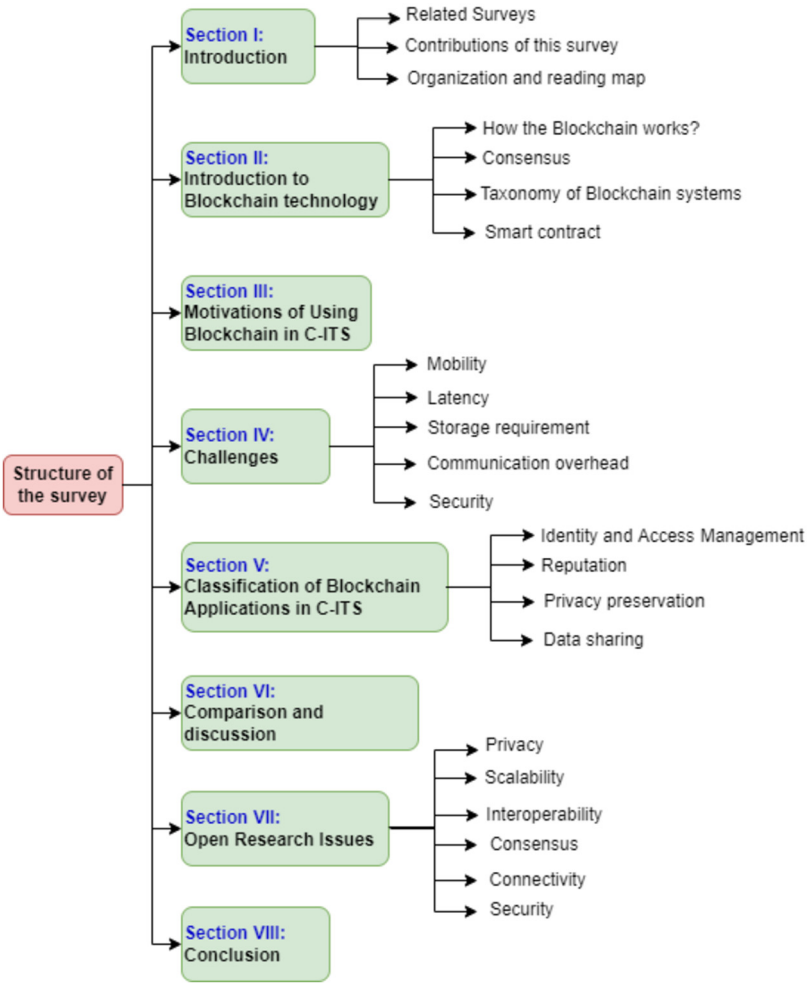


Fig. 2. Organization of the paper.

blockchain technology into vehicular networks. Section 4 describes major challenges in implementing blockchain in C-ITS. Section 5 presents an overview of the recent works on blockchain-assisted vehicular applications. Section 6 introduces a comparison of the discussed papers. In Section 7, we highlight some open research issues. Finally, in Section 8, we conclude the paper. The structure of this survey is also depicted in Fig. 2. Additionally, to assist the readers, a list of major abbreviations used in this survey is provided in Table 2.

2. Introduction to blockchain technology

Before reviewing the state of the art on blockchains in C-ITS, it is necessary to introduce several basic concepts on blockchain technology. Hence, in this section, we will give a brief background on blockchain operation, consensus algorithms, and the smart contract concept.

A blockchain [24] is defined as a distributed database (ledger) that stores permanent and immutable records of transactional data linked together by a chain of blocks. A blockchain is a fully decentralized system based on a peer-to-peer network. Each node in the network keeps a copy of the ledger to avoid having a single point of failure. All copies are updated and validated simultaneously.
Although the initial objective of creating the blockchain was to solve the problem of multiple spending in crypto-currency (virtual money), the technology has been later explored in many use cases as a secure way of managing and protecting any kind of data (monetary or not).

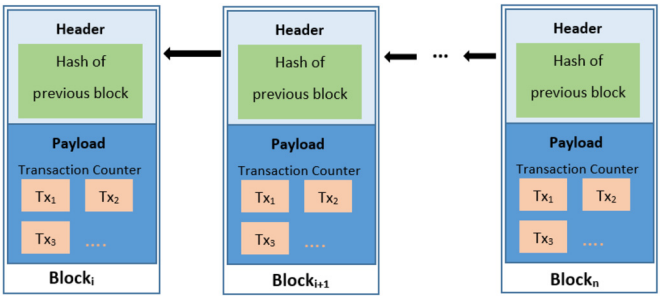


Fig. 3. The structure of a blockchain.

As shown in Fig. 3, a ledger is composed of a set of blocks. Each block contains two parts. The first part is the *header* of the block. It contains information about the block such as the *timestamp*, the *hash of the transactions*, as well as the *hash of the previous block*. The second part represents the *payload* of the block. It contains the recorded *transactions* in the block. These transactions can be monetary data, medical or industrial information, or traffic road data for the vehicular network use case.
All the existing blocks form a chain of linked and ordered blocks. The longer the chain, the more difficult it is to falsify. Indeed, if a malicious user wants to modify or exchange a transaction on a block, it must, first, modify all the following blocks, since they are linked by their hashes. Then, he must change the copy of the blockchain stored by each participating node.

Table 2
List of abbreviations used in the survey.

Notation	Meaning
C-ITS	Cooperative Intelligent Transport Systems
ITS	Intelligent Transport Systems
V2X	Vehicle-to-Everything
BC	BlockChain
IoT	Internet of Things
VANET	Vehicular AdHoc Networks
RSU	Road-Side Unit
PoW	Proof of Work
PoS	Proof of Stake
DPoS	Delegated Proof of Stake
PBFT	Practical Byzantine Fault Tolerance
PoET	Proof of Elapsed Time
PoA	Proof of Authority
IPFS	Inter Planetary File System
MEC	Mobile Edge Computing
IAM	Identity and Access Management
CA	Certification Authority
RA	Revocation Authority
CRL	Certificate Revocation List
V2I	Vehicle to Infrastructure
IoV	Internet of Vehicles
VCS	Vehicular Communication Systems
SM	Security Manager
PKI	Public Key Infrastructure
IVTP	Intelligent Vehicle Trust Point
PIR	Private Information Retrieval
RHS	Ride-Hailing Services
SPs	Service Providers
TA	Trusted Authority
CAV	Connected and Automated Vehicles
AV	Autonomous Vehicles
DoS	Denial-of-Service
DSRC	Dedicated Short-Range Communications

2.1. How the blockchain works?

The working principle of blockchain is explained in Fig. 4. It consists of six main phases:

- First, a user sends a new transaction
- Then, the transaction is broadcast on the P2P network
- Next, all network nodes check the validity of the transaction based on a consensus algorithm
- After that, a new block is created once the transaction is validated
- Then, this new block is permanently and immutably appended to the blockchain
- Finally, the new transaction is completed

The word transaction presented here is suitable for any type of application.

2.2. Consensus

Consensus protocols are one of the most important and revolutionary aspects of blockchain technology. It means that the nodes in the network agree on the same state of a blockchain, making it a sort of self-auditing ecosystem.
In fact, each node in the network can submit information to be stored on the blockchain. Thus, it's important that there is a review and a confirmation step, in the form of a consensus on whether to add or not that information to the blockchain.
Therefore, consensus algorithms are an absolutely crucial aspect of blockchain technology and are basically designed to fulfill two main functions. First, consensus protocols allow a blockchain to be updated, while ensuring that every block on the chain is true and keeping participants motivated. Second, it prevents a single entity from controlling or derailing the entire blockchain system. The goal of consensus rules is to ensure that a single chain is used and followed.
In the existing blockchain systems, a number of consensus mechanisms are used, mainly, Proof of Work (PoW) [24], Proof of Stake (PoS) [25], Delegated Proof of Stake (DPoS) [26], and Practical Byzantine Fault Tolerance (PBFT) [27]. Here we will explore how these systems work and the differences between the different protocols.
Proof of Work (PoW) [24] is a consensus protocol introduced by Bitcoin and widely used by many other crypto-currencies.
The process of the PoW algorithm is known as mining and the nodes in the network are known as "miners". The PoW comes in the form of an answer to a mathematical problem, which requires considerable work but is easily verified once the answer is obtained. The only way to solve these mathematical puzzles is through nodes on the network, performing a lengthy and random process of presenting answers on a trial-and-error basis. To accept a block, the answer must be a number less than the hash of that block.
A miner continues to test different unique values (known as *nonce*) until an appropriate value is produced. This *nonce* is tested by the other nodes to determine whether it is the solution to the hash puzzle or not. When the *nonce* verification is successful, the node appends the new block to its locally stored blockchain and starts processing the new block.
The winner of the cryptographic puzzle must have expended considerable energy and crucial processing time to find the *nonce* and gain the ability to create new blocks in the blockchain. Therefore, he is usually rewarded for his work. The reward for such actions depends on the blockchain itself. In a Bitcoin blockchain, the winner will be rewarded with a bitcoin (i.e., the crypto-currency of the Bitcoin blockchain).
Despite some merits, the proof of work is considered an imperfect consensus protocol, especially considering the amount of energy consumed in running the protocol. Therefore, alternative consensus mechanisms [28] have been implemented, in order to address this issue and enhance the blockchain process.
Proof of Stake (PoS) [25] is a consensus algorithm that relies on the crypto-currency of the blockchain user. In a Proof of Stake system, the creator of the next block is determined by a random system that is, in part, dictated by how much crypto-currency a user holds or, in some cases, how long they have held that particular currency. The randomness in a PoS system prevents centralization, otherwise, the richest individual in the system would always create the next block and would constantly increase his wealth and therefore his control of the system. The main advantage of Proof of Stake, compared to a system such as PoW, is that it consumes considerably less energy and is, therefore, more cost-effective.
Delegated Proof of Stake (DPoS) [26] is a voting algorithm where stakeholders assign their work to a third party. In other words, they can vote for a few delegates who will secure the network on their behalf. The delegates are responsible for reaching a consensus when generating and validating new blocks. The number of votes is proportional to the number of coins held by each user, i.e. stakeholders with more coins get more votes. However, a delegate must get the most votes from various stakeholders and only the top twenty delegates are eligible to perform the stated functions. This factor in itself creates efficiency, as it puts pressure on delegates to perform their jobs perfectly, as they can be replaced in any case where they misbehave or act fraudulently.
The Practical Byzantine Fault Tolerance (PBFT) consensus introduces new concepts of replication in order to ensure system continuity and reliability even in the presence of arbitrary behavior [27]. The assumption is that the total number of misbehaving nodes should not equal or exceed 1/3 of all nodes in the network. A new block is created in one turn. Indeed, a lead node

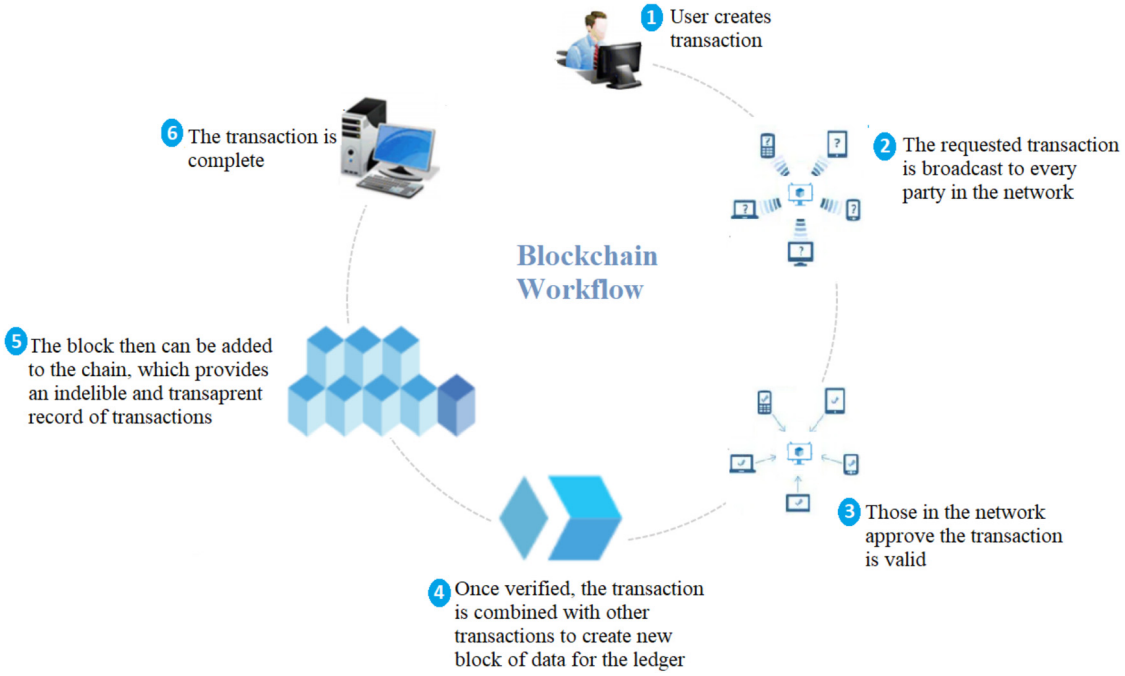


Fig. 4. Working flow of Blockchain.

Table 3
Comparative table of the main consensus mechanisms.

Consensus	PoW	PoS	DPoS	PBFT
Type of Blockchain	Public	All Types	Public	Private/Consortium
Transaction throughput	Low	High	High	High
Energy consumption	Yes	No	No	No
Network Scalability	High	High	High	Low
Security level	Very High	Low	High	Medium
Decentralization level	Medium	High	Very High	Low

is selected according to some requirements for each turn. This node is in charge of the sequence of the transaction. Next, the entire process can be split into a pre-preparation stage, a preparation stage, and a validation stage. Then, at each step, a peer moves on to the following step if it has been approved by more than two-thirds of the whole set of nodes. Therefore, PBFT requires that each node be known to the network. Hence, as more participants reach the PBFT consensus, the system becomes more secure. Table 3 presents a summary comparison of the consensus mechanisms discussed throughout this subsection. This comparison was made on the basis of all the issues relating to these mechanisms: type of blockchain, energy consumption, security level, decentralization level, transaction throughput, and network scalability.
Recently, several research studies have been conducted to enhance the existing consensus algorithms. Such attempts include Proof Proof of Elapsed Time (PoET) [33], Raft [35], Ripple [30], Proof of Authority (PoA) [32], Tendermint [31], and kafka [34]. A wider survey of recent consensus protocols can be found in [29], [36].

2.3. Taxonomy of blockchain systems

Based on the targeted use case and its specific requirements, blockchains have been classified into *permissionless* blockchain and *permissioned* blockchain.
Within a *permissionless* blockchain, nodes can freely join and leave the network [37]. A permissionless blockchain presents a **public** network that allows anyone to join the blockchain system and be part of it. Therefore, it is a distributed ledger system without authorization and without restrictions. Examples of existing public blockchains include Bitcoin [24], Ethereum [38], and Litecoin [39].

Differently, within a *permissioned* blockchain, access to the ledger data and participation in the consensus process are restricted only to authorized participants. An example of the permissioned blockchain is the **private** blockchain, which is functioned only in a closed network and is restricted to particular participants. This type of blockchain is used for individual members to operate the system network. More specifically, it is employed within a company or organization that plans to use the blockchain only for its own internal purposes. Furthermore, **consortium** blockchain is considered as a permissioned blockchain, this type of network hybridizes the public blockchain with the private blockchain, therefore, there is more than one central manager for the system. In addition, access and provision of read, write and audit privileges to the blockchain are managed by multiple organizations. Multichain [40], Hydrachain [41], Hyperledger Fabric [42], Corda [43], and R3 [44] are examples of a permissioned blockchain.
In the following, we compare these three types of blockchain, namely *public*, *private*, and *consortium* blockchains based on different criteria. The comparison is summarized in Table 4.

- **Access permission:** For the public blockchain, anyone can access the data, and submit transactions that are actually verified. In contrast, in the private blockchain, the block with both write and read permissions is controlled by an organization, and access is restricted. While the consortium blockchain can enable everyone or only attendees to gain access. Hence, it can embrace a hybrid access approach.
- **Decentralization:** Since the public blockchain operates in an open network where any individual can be a member, thus this type of blockchain will be fully decentralized. In the con-

Table 4
Comparison of public, private and consortium blockchains.

Features	Public	Private	Consortium
Accessibility	Read/write for anyone	Read/write for a single organization	Read/write for multiple selected organizations
Decentralization	Decentralized	Partially decentralized	Partially decentralized
Consensus determination	All miners	Selected set of nodes	Selected set of nodes
Transaction speed	Slow	Lighter & Faster	Lighter & Faster
Efficiency	Low	High	High
Immutability	Nearly impossible to tamper	Could be tampered	Could be tampered

sortium blockchain, the network is managed by several organizations or companies, which allows this type of blockchain to be partially centralized. However, it is found that only one group of organizations is responsible for controlling a private blockchain, hence this type of blockchain is fully centralized.

- **Transaction speed:** Obviously, a transaction takes less time in a consortium or a private blockchain than in a public blockchain. Indeed, the transaction speed of the public blockchain is slow because this network takes time to reach consensus.
- **Efficiency:** For a public blockchain, the propagation of transactions and blocks takes a long time because there are numerous participants. Therefore, there is a high latency and a limited throughput for transactions. With few participants, a private or consortium blockchain could perform better.
- **Immutability:** In a public blockchain, the data is stored among several distributed participants, therefore it is virtually impractical to alter this data. However, in the case of private or consortium blockchain, if the controlling organization or the majority of the consortium wants to modify the data, the blockchain could be modified.

2.4. Smart contract

A Smart Contract [45] is simply lines of code that facilitate, check and run the negotiation or execution of a contract. They are typically saved on a blockchain ledger and automatically run when predefined requirements are satisfied. A smart contract is usually employed for automating agreement execution. They are most obvious in enterprise collaborations, where all shareholders can be sure of the result, without the intervention of an intermediary or time loss.

3. Motivations of using blockchain in C-ITS

In the past few years, the Cooperative Intelligent Transportation Systems (C-ITS) aim to improve the safety of road users and agents working on the road network, to facilitate traffic management, by delivering real-time information to drivers and managers of roads (e.g., obstacles on the road, work in progress). They are based on digital interactions between vehicles, vehicles, and infrastructure. Today's vehicles are more than just a means of transportation, they are also embedded with a wide variety of sensors that provide important data. Actually, there is continuous data collection in the vehicular environment. Therefore, managing a huge amount of information and providing a real-time reply is a tremendous challenge. Moreover, owing to the open environment in the wireless network, several issues raised and need specific consideration [46], including integrity, privacy, heterogeneity, and communication. These main challenges are summarized as follows:

- **Integrity:** Gathering and analyzing data can contribute to effective road safety and improve the traffic management of the vehicular network. Hence, a non-authorized alteration of the data could result in dire outcomes, thus preserving data reliability and integrity is of paramount concern.
- **Privacy:** Privacy information, such as the user's real identity and actual location, represents sensitive data in the communication flow. Therefore, it is necessary to guarantee the preservation of this private information and to protect them from being lost [47]. Furthermore, during communication whether with vehicles or infrastructure, users should decide what information should be exchanged and what information should remain private.
- **Heterogeneity:** The C-ITS enables the various entities of the network to exchange and interact with each other via the Internet. These entities have heterogeneous features, including hardware and software devices, communication standards, operating systems, etc. For this reason, the application of a decentralized technology such as blockchain technology guarantees a certain fluctuation in the application's complexity and the number of devices connected in a vehicular system.
- **Communication:** Vehicular networks are susceptible to several types of attacks owing to their inherent properties, especially high mobility with frequent disconnections. Indeed, the communication link between vehicles is frequently broken in C-ITS, due to the dynamic change of the network topology. In particular, communication connections among opposing vehicles are restricted to only a few seconds, which leads to frequent disconnection events. As a result, vehicles can communicate with each other for a very short duration. Therefore, the network will be more susceptible to attacks, and it will be hard to identify suspicious vehicles.

As a rising technology, blockchain offers several advantages, including decentralization, trust, pseudonymity, immutability, traceability, transparency, and security. The above advantages led to the enhancement of C-ITS applications. Briefly, the unique values of blockchain can be summarized as follows:

- **Disintermediation:** The blockchain ledger is not held by a single individual, business, or organization, but by all participating network computers spread across the globe. This allows two parts of the vehicular network to interoperate with no requirement for a trusted third party to validate operations or check the veracity of records.
- **Immutability and Transparency:** Once data is added, it cannot be changed or lost, which provides an incorruptible historical record that will be permanent in the system. In addition, transparency is provided as all changes are mirrored on the ledger and can be verified by any stakeholder in the network. Thus, blockchain-based C-ITS systems and applications are characterized by strong immutability. In fact, the integration of blockchain in a vehicular network helps to avoid falsification or modification of the exchanged data and to enable accurate auditing. Additionally, it can enhance the transparency of the vehicular network.
- **Availability:** By synchronizing and replicating blockchain records across all stakeholders in the network, security risks such as disruption, single point of failure, and availability threats become manageable. Indeed, the implementation of blockchain in the vehicular network allows C-ITS services to function

properly even when one or multiple participants are compromised.

- **Auditability and Traceability:** C-ITS entities can communicate with any peer in the distributed system to check and track previous records, as every record on the blockchain is validated and stored with a unique timestamp. Therefore, the auditability and the traceability of the data saved and shared in the blockchain-based vehicular network is greatly improved.
- **Trust:** Data sharing between trusted parties is very critical for large-scale C-ITS applications. However, vehicular networks connect heterogeneous entities that may not be trusted. Therefore, by using consensus mechanisms, transactions will be added to the blockchain ledger only when most of the participants approve them. These transactions are then placed on the blockchain and made available to all the network peers.
- **Anonymity:** There is no requirement for the user's real identity in the data exchange and transaction creation in a blockchain network. Where each sender needs to be aware only of the receiver's blockchain address. Therefore, each user in the vehicular network is allowed to participate in the blockchain system only with his address. Thus, the real identity of users will be protected, resulting in "anonymity". However, a malicious vehicle can spread wrong traffic information to coerce other entities into taking incorrect decisions. Thus, malicious users' identities ought to be traced in anonymous advertisements.

4. Challenges

The employment of blockchain technology for Cooperative Intelligent Transport Systems leads to several benefits. However, the integration of blockchain technology is certainly not smooth sailing, and the implementation of blockchain within vehicular networks may also face many challenges. In this section, we discuss the major challenges faced in implementing blockchain-based applications for C-ITS, including node mobility, blockchain latency, storage requirements, communication overhead, and security issues.

4.1. Mobility

The mobility of nodes has an undesirable effect on the performance of a blockchain-based vehicular system. In fact, the dynamic topology induced by the movement of vehicles leads to common road perturbations, poor route convergence, and low transmission rates. In addition, mining presents the primary task for transaction validation and block creation in a blockchain-based system [48]. The previous literature on mobile blockchain [49–51] assumes that miners need to communicate among themselves to validate and store new blocks in the blockchain. Moreover, due to the random nature of the wireless network and the dynamism of the vehicular environment, the network participants are incapable of maintaining stable network communication. As a result, these participants are unable to reach a consensus and validate blocks correctly. Kim et al. [51] analyzed the effects of mobility on blockchain-based vehicle networks and assessed its performance in terms of rendezvous stability, successful addition of blocks, and the number of blocks allowed to be traded during the rendezvous. The results of this study reveal that when nodes move at a low velocity the rendezvous period is longer and then the number of blocks successfully added increases, however when nodes move fast, the rendezvous period is shorter and the number of added blocks decreases accordingly.

4.2. Latency

In a blockchain system, latency is defined as the time required to transmit and confirm a transaction by the network participants. A faster response is the key requirement for several real-time applications in C-ITS such as safety messages for traffic management, for example; to prevent road crashes, real-time warnings about traffic conditions need to be provided to road users [52,53]. Hence, this type of urgent event requires a fast response time. Moreover, low latency is the fundamental requirement for several real-time applications in future C-ITS. Actually, to calculate system latency, we need to consider the processing effort as well as the total time taken to execute a task. Whereas to estimate the consumed energy we have to look at the required power to perform this task.
Since the execution time of the proof of work consensus depends on the complexity of solving a puzzling problem, this consensus requires a huge energy and time consumption. Therefore, the validation cost of PoW-based transactions is high, which leads to a delayed response system [54]. Besides, as Bitcoin is a PoW-based technology, it faces several issues related to high transaction latency and low transaction throughput performance [55]. For instance, in Bitcoin, the average time to generate a block is 10 minutes [56]. Therefore, Bitcoin is too slow for delay-sensitive C-ITS applications. Furthermore, the number of transactions per block is also a critical factor that negatively impacts the latency of a blockchain-based C-ITS. Therefore, the latency and the overhead of a vehicular network depend on the number of processed transactions and the required time to validate these transactions.

4.3. Storage requirement

Another challenge inherent to the deployment of blockchain in C-ITS is storage capacity limitation. Actually, a large amount of information needs to be exchanged and processed by the different vehicular network entities. However, the blockchain system requires each peer of the network to process all transactions and keep track of them until the first block. Accordingly, it is very difficult to directly employ blockchain technology in vehicular network environments in which both vehicles and RSUs are constrained in terms of storage resources [57]. Therefore, it is essential to study where the data will be saved, i.e. on or off the blockchain, as well as how the data will be saved in such resource-constrained entities. To overcome the limitation of the resources, cloud systems have hugely been deployed. For example, the authors in [58], [59] have proposed using cloud-based storage to store all the transactions of the system. However, the cloud can greatly increase the time required for communication in these applications, which leads to significantly worse response time [60]. Another solution to address the storage capacity limitations is the incorporation of the Inter Planetary File System (IPFS) with the blockchain technology [61]. IPFS is a distributed file storage system that produces a hash of the recorded data. Currently, this system is used in such vehicular applications based on blockchain technology [62], where the network validators (RSUs) store the data hashes in the blockchain ledgers while the details of these data are stored in IPFS. However, as mentioned in [63], the limited bandwidth of the IPFS system leads to some scalability issues. Moreover, IPFS has a few notable weaknesses [64], such as resolution and download bottlenecks, as well as high latency for input/output operations.

4.4. Communication overhead

The communication overhead can be defined as the time cost required to generate an amount of data or to transmit a quantity of data among the network entities. In the case of using cloud services as a storage solution, once a vehicle would like to check

the accuracy of the received information, the verification process is made through the cloud. One main disadvantage of this approach is that it relies on continuous communication with the cloud, which adds significant overhead to the network [60].
To address this issue, some researchers have proposed to incorporate a Mobile Edge Computing (MEC) model into blockchain-based C-ITS architectures [67], [68], [69]. MEC is a new emerging model that can be integrated with infrastructure at the edge of the network. For example, within the RSUs for vehicular environments, to support the computation, storage, and sharing of massive amounts of vehicle data. Edge computing reduces transport time and improves data availability by inserting computing power and storage capacity directly at the network edge [66], which results in an enhancement of the network response time and communication latency [65].

4.5. Security

Vehicular networks are susceptible to many kinds of security attacks as they operate in an open and dynamic environment. Particularly, the security of the main network entities, namely infrastructure, and vehicles, is a very challenging task. In fact, Roadside Units (RSUs) and vehicles cannot be fully trusted and thus may result in serious security and privacy challenges for blockchain-based applications in VANET [70]. Among these issues, we can cite the minor voting collusion problem, in which collusion between the blockchain nodes (such as RSU) may lead to the election of a malicious miner who can falsify legitimate transactions during the mining process. Moreover, during the block verification step, the collusion of miners may create false results in the blockchain and lead to block verification collusion. Broadly, once compromising a blockchain node, an attacker can append, remove, and falsify the stored data easily.

5. Classification of BlockChain applications in C-ITS

Recently, several blockchain-based applications have been proposed in the vehicular environment. In this section, we thoroughly review the state of the art of blockchain-based solutions for vehicular networks. As shown in Fig. 5, we categorize these solutions into four main categories:

- Identity and Access Management: Identity and Access Management (IAM) comprises all the processes to handle a user's identity in the network. It is principally a matter of authenticating participants on the network and ensuring the traceability of their access rights on the network, here we refer to authorizations. In vehicular networks, it is important for all participants to be identified, authenticated, and authorized correctly when accessing data and applications, without sacrificing the privacy of credentials. Traditional systems, rely on a centralized model that uses a single trust node where the IAM process is managed by a central entity. As a result, all participant authentication data, i.e. keys and certificates, are saved in the database of the Certification Authority (CA), which poses a single-point-of-failure problem. Using blockchain on the vehicular network for IAM is a growing area of research. Indeed, different vehicular models based on blockchain technology have been investigated by researchers, to secure the authentication information, manage and automate access rights with smart contracts, and implement a vehicular system that does not require a trustworthy entity such as a central CA. Some of these approaches are discussed below in section 5.1.
- Reputation: The recent development of Cooperative Intelligent Transport Systems (C-ITS) has led to new responsibilities that require a focus on the reputation mechanisms needed to build trust among network stakeholders. However, since vehicles are anonymous and frequently change their pseudonyms, it becomes very difficult to maintain their reputation history. Therefore, considerable effort has been made to develop blockchain-based reputation systems for C-ITS to address these issues. Some of these approaches are described below in Section 5.2.
- Privacy preservation: Users' data privacy preservation is an open issue in C-ITS. Users are paying more and more attention to their private information in the data era. Therefore, it is very important to protect vehicular identity and location privacy in a vehicular environment. Furthermore, it is crucial to guarantee the privacy of a user, in order to ensure that the information is not leaked. Consequently, to address privacy concerns, blockchain technology uses the pseudonym technique to preserve privacy and hide the real identities of vehicles. Hence, several solutions have been proposed as presented in Section 5.3 to ensure the privacy of users using blockchain technology.
- Data sharing: A primary goal of the vehicle network is to communicate vehicles with each other, in order to announce incidents like crash information, emergency warnings, congestion information, climate reports, etc. Since the blockchain is an immutable and shared ledger for storing transactions, it provides a seamless and auditable way to record this information. Moreover, blockchain technology can be employed to store information related to vehicles (i.e., distance traveled, accident history, owner history, service history, etc.). In fact, blockchain's traceability and immutability characteristics can be used to identify wreck and mileage fraud. In section 5.4, we detail some works that incorporate blockchain technology within C-ITS for data-sharing applications.

5.1. Identity and access management

In order to ensure that users cannot illegally access or attack the network, identity management and access authentication are essential for C-ITS security. It is therefore critical to assure that only authenticated vehicles can interact with the network and that revoked vehicles do not interfere with the communication.
In addition, enabling a quick authentication between fast-moving vehicles and managing participants' access rights in the network are complex tasks that are not efficiently addressed by traditional IAM solutions mainly due to the single point of failure problem and the high cost of computational and communication overhead in the network induced by the reliance on a single trusted party. Hence, there is a real need to search for a better-suited IAM solution for C-ITS. In this direction, blockchain technology could be a good candidate mainly to its decentralized and distributed architecture. In addition, as this technology provides data immutability, thus it will enhance the system automation and integrity. In this context, a large body of work has been proposed in the literature to assess identity and access management in vehicular networks using blockchain.
Shiver et al. [71] developed a decentralized ride-sharing architecture implemented on the Hyperledger Fabric[1] blockchain platform. The authors have implemented the ride-sharing architecture using two organizations that act as both endorsing peers and committing peers, an ordered node, a certificate authority, and then multiple user accounts which are utilized by the client application to

[1] Hyperledger Fabric can be seen as a project within Hyperledger's blockchain platform. It is basically an open-source platform for blockchain development launched in 2015 by the Linux Foundation.

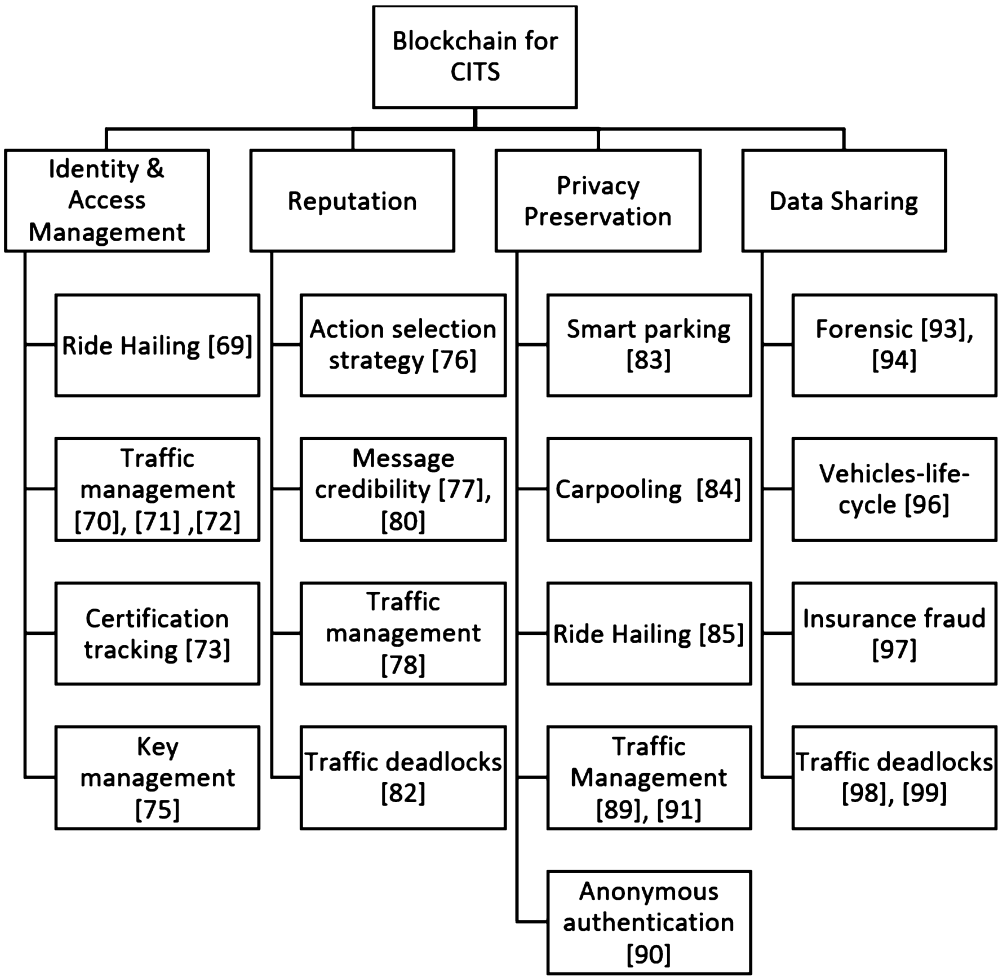


Fig. 5. Classification of blockchain-based C-ITS applications.

register drivers and riders. Endorsing peers send transaction proposals from driver and rider client applications in the network and return signed proposal responses. This platform serves so as an intermediary connecting drivers and passengers. The authors used blockchain technology to guarantee trust between several untrusted entities. In particular, they employed a chaincode[2] Using this protocol, information is provisioned only to the concerned users and applied via an access control implicitly realized in the chaincode functions. In addition, their proposal allows user certification to be implemented independently of a centralized certification authority. This is due to the assumption that each organization uses a certification authority to manage user identification (including drivers and passengers). Finally, they evaluated their proposal by running a static analysis tool and analyzing the performance under a high network load. However, other framework enhancements may be added, such as more chaincode functionality (e.g., reputation system, designated driving zones).

In [72], Malik et al. have introduced a blockchain-based vehicle authentication and revocation scheme. The proposed model not only provides vehicle authentication by alleviating the reliance on a trusted authority but also quickly maintains the revocation status of vehicles in the blockchain. In the suggested framework, users get their pseudo-identities from the CA, which are kept in the immutable blockchain ledger with their certificate, and the corresponding pointer to the ledger entry allows RSUs to check the vehicle's identity. A private blockchain is employed to ensure restricted access to the ledger. The ledgers are fully controlled by the Revocation Authority (RA) and the Certification Authority (CA), RSUs have the rights to read only, whereas vehicles have no rights. This avoids any risk of exposure to unreliable entities. This framework does not employ a PoW mechanism, which reduces computational costs. They used Proof of Authority (PoA), where access privileges are given based on a predefined authority. In addition, the proposed scheme facilitates the discovery of a node's revocation in a single, quick step, and eliminates the requirement for any Certificate Revocation List (CRL). The design of this system maintains vehicle privacy but does not address communication security.

In [73], Ali et al. have proposed an effective Certificate-Less Public Key Signature (CLPKS) scheme based on bi-linear matching to provide conditional privacy-preserving authentication for Vehicle to Infrastructure (V2I) communication in VANETs. The authors employed blockchain technology in their solution to effectively implement transparency of pseudo-identity revocation before signature verification. Furthermore, to speed up the checking process, CLPKS aggregates the functions of signature verification and enables batch signature verification. In addition, the CLPKS system achieves higher protection and security against various attacks with lower computational costs. However, the design of the Certificate-Less Signature scheme for V2V communication is required.

Zheng et al. [74] have proposed a decentralized traceable Internet of Vehicles (IoV) system based on blockchain technology. The

[2] In Hyperledger Fabric, chaincode is the "smart contract" that executes on peers and generates transactions.

proposed scheme implements secure access between vehicles and RSUs. The proposed system ensures anonymous communications. Vehicles can use pseudonyms for V2V and V2I communication without disclosing their real identities. The proposed scheme contains five stages: (1) system initialization, (2) vehicle registration, (3) vehicle authentication, (4) vehicle announcement, and (5) messages forwarding. In the initialization phase, the participants prepare to be occupied with numerous domain parameters required for security operations. In the registration phase, the certification authority generates a series of system parameters according to the unique ID provided by the registered vehicle. In the vehicle authentication phase, as soon as the vehicle is active on the road, it authenticates with RSU. In this proposal, the RSUs as peer nodes build the blockchain network. In the announcement of the vehicle phase, the RUS verifies the integrity of the event announced by the vehicle and does not verify the identity of the sender, because only the authenticated vehicle can declare the traffic conditions. If the result is valid, the RSU packs up a new transaction. Finally, in the forwarding phase, the vehicle can choose whether to forward the transaction or not after checking the authenticity of the transaction about the road event. This solution allows a transparent authentication and advertisement between the entities of the network, which is realized due to the use of blockchain technology. Moreover, with the help of CA and RSU, the system guarantees conditional privacy in order to retrieve the true vehicle identity that misbehaves in the anonymous advertisements. Finally, only the hash value of the event transaction is appended to the blockchain, the real details of the events are stored in the cloud server.

In order to monitor the membership status of vehicles, Lasla et al. [75] proposed the use of blockchain technology to maintain a record of each vehicle's certificate (valid or revoked) in distributed and immutable ledgers. Essentially, they replaced certificate verification with a lightweight blockchain-based authentication scheme. In the proposed scheme, RSUs act as validators, while authorities[3] and vehicles are able only to read or transmit transactions for validation. Moreover, by verifying the digital signature and the sender's public key, the integrity of the message is confirmed. In fact, each vehicle authenticates the message by checking whether the sender's public key is present in the blockchain and whether it is valid. Moreover, this solution implements additional security mechanisms to detect and revoke misbehaving vehicles. However, to evaluate the performance of their proposal, the authors employed Bitcoin technology. The Bitcoin system is based on the PoW consensus, which requires high computational power to add new blocks [55].

In Vehicular Communication Systems (VCS) the security of exchanged vehicular messages is the primary focus. Hence, to address this issue, a secure key management scheme is required [76]. To reduce the key transfer time, the authors of [77] proposed a new model to achieve secure key management in the heterogeneous network using key transfer between two different networks and a dynamic key management system as illustrated in Fig. 6. Moreover, in order to improve the performance of their system, the authors proposed to simplify the key exchange procedure, by removing the tiered authorities (central managers) in the blockchain-based scheme. The key exchange processes are checked and validated by the Security Manager (SM)[4] network. As shown in Fig. 7, by using the simplified structure, the exchange of messages across security domains can be accelerated as the message is sent directly to the destination rather than through central handlers. In addition, the period of transaction collection can dynamically change according to different traffic levels. Finally, simulations prove that the proposed blockchain-based outperforms existing central manager-based systems.

Summary As shown in Table 5, several applications based on blockchain for identity and access management have been implemented for vehicular networks. Most of the proposed solutions use blockchain in IAM applications due to its immutability. In fact, blockchain is employed to store vehicle information, namely, identity, pseudonyms, and the correspondence between the real ID and the pseudo-ID [72], [74]. Indeed, owing to the structured hash of the blockchain data, any kind of modification made to this data can be detected automatically. Furthermore, as a blockchain stores the data within immutable, transparent, and distributed records, we can easily monitor the vehicle's membership status. In other words, blockchain can be employed to check whether the vehicle's certificate is valid or not (revoked) [75], [73] in order to accelerate the verification process. In fact, instead of verifying certificates stored in the cloud, entities can check locally the blockchain. Moreover, if the verification is based on pseudonyms instead of certificates as in [72], unlike the traditional Public Key Infrastructure (PKI)) system, the vehicle sends to the RSU the index of the pseudonym transaction instead of issuing a certificate. Then the RSU would check the blockchain, which would speed up the lookup process. Other studies proposed to use blockchain to eliminate the presence of a third party [71], [77]. They take the merits of blockchain which is to establish trust between non-trusting participants Besides, we notice that we can speed up the exchange of messages in the VCS, by sending the message directly to the destination instead of going through the central managers.

5.2. Reputation

The reputation of a vehicle is based on its behavior as well as the history of the type of data that it supplied to the network. Blockchain technology enables to store permanently the reputation scores in a tamper-proof ledger, that cannot be alerted by attackers. Therefore, there are a number of research works with respect to the trust or reputation of vehicles. For example, in order to assess the dangerous level of each vehicle, Dai et al. [78], proposed an indirect reciprocity security scheme with an assigned scalar reputation. In fact, vehicles will save and share their trust level rather than saving and sharing vehicular data on the blockchain. The trust level (reputation score) is derived using the principle of indirect reciprocity, where the reputation of a node is increased if it assists other nodes and decreased if it fails to assist other nodes. Then, each entity in the network uses this score to verify the authenticity of the message sender. However, to examine the effectiveness of this system for authenticating vehicles, the processing and storage overhead of applying the reputation score on the blockchain has not been considered. In addition, it will be more difficult to reach a consensus and add new blocks to the blockchain as more vehicles join this system. Yang et al. [79] have implemented a novel reputation system using blockchain technology for data credibility assessment. In this paper, the author has classified the different entities into four types:

- Trusted authority: responsible for the registration and for the issuance of the capacity certification of a vehicle.
- Ordinary vehicles: broadcast messages, generate ratings and receive validated rating packages.
- Malicious vehicle: Any vehicle that has broadcast fake message/rating.

[3] In reality, the function of authorities, is to confirm whether a vehicle meets the requirements for membership (e.g., the Department of Motor Vehicles, insurance companies, manufacturers, etc).

[4] SMs are at the top level of the VCS to handle the cryptographic tools. Each SM has its unique zone of logical coverage, which is known as the security domain.

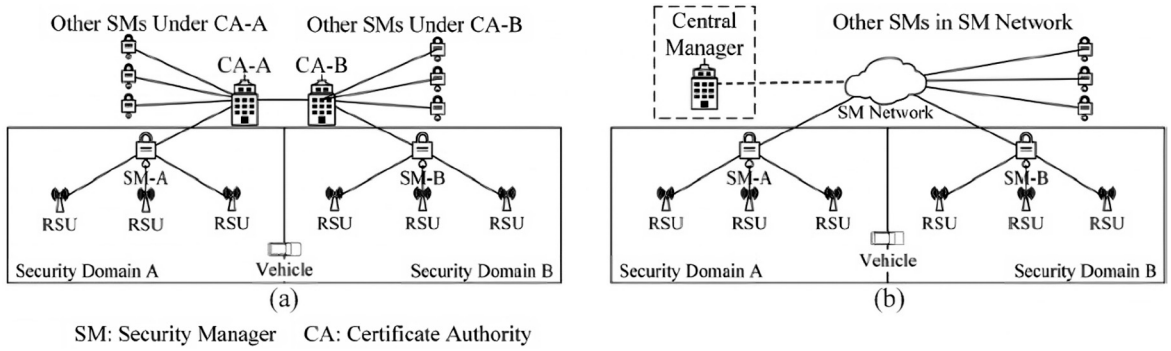


Fig. 6. Network frameworks [77]. (a) Traditional framework with third-party authorities. (b) Blockchain framework excluding third-party authorities.

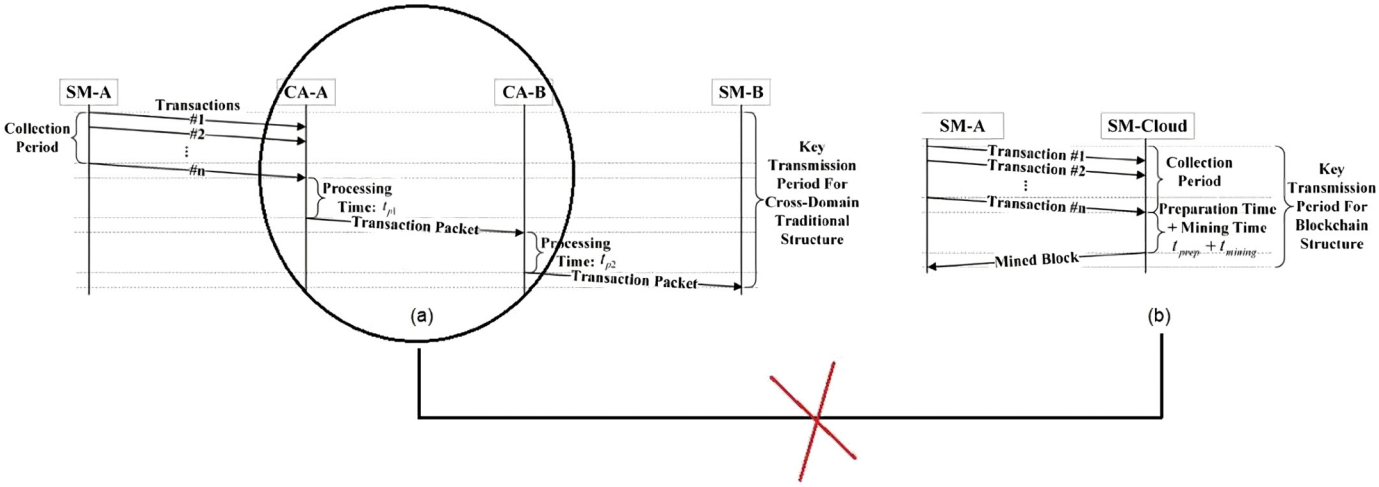


Fig. 7. Key transfer handshake procedures [77]. (a) In traditional structure with third-party authorities. (b) In blockchain structure excluding third party authorities.

Table 5
Comparison of identity & access management solutions.

References	Applications	BC Function	BC Type	BC Technology	Consensus	BC Participants	Smart Contract	Evaluation	
								Simulation/ Experimentation	Metrics
[71]	RideHailing	Trust, Disinter-mediation	Consortium	Hyperledger Fabric	kafka	Driver, Rider	X	Experimentation	- Constant Rate Network Traffic - Poisson Distribution based network traffic - Organization Restructuring Tests
[72]	Traffic management	Immutability, Disintermedia-tion	Private	Bitcoin	PoA	CA, RA, RSUs		Simulation	- Delay performance between the OBUs and RSUs - Throughput and PDR with respect to the number of vehicles
[73]	Traffic management	Immutability, Transparency	N/A	N/A	N/A	TRA, KGC, RSUs, Vehicles		Experimentation	- Computation cost - Communication cost
[74]	Traffic management	Trust, Immutability	N/A	N/A	PoW	RSUs, Vehicules		Experimentation	- Time cost for ach part of the proposal
[75]	Certification tracking	Immutability, Transparency	Public	Bitcoin	PoW	Authorities, RSUs, Vehicles Vehicles		Simulation	- The average required time to lookup for a transaction
[77]	Key management	Disintermedia-tion, Transparency	Public	Bitcoin	PoW	Central managers, Security managers, Vehicles, RSUs		Simulation	- The processing time in terms of transactions

- Miner: responsible for generating a rating block and broadcasting the block to other vehicles.

In the proposed model, the vehicle evaluates incoming messages based on the observation of the traffic environment and aggregates these evaluations into a block. A miner is in charge of disseminating its evaluation block to the other vehicles. Upon the scores recorded in the ledgers, the vehicles compute the reputation value of the transmitter and then assess the trustworthiness of the message. The system does not store traffic information and privacy preservation methods are not presented. Moreover, with more vehicles joining the system, it will be difficult to reach a consensus for appending new blocks. Finally, implementing a blockchain with proof-of-work consensus requires a high cost, hence it is very difficult to implement in resource-constrained vehicles. Shrestha et al. [8] introduced a blockchain-based system to store node reliability and message reliability to be used as proof of truth by other vehicles. There are two phases for this blockchain system, namely, the broadcast phase and the mining phase. In the broadcast phase, a vehicle broadcasts a message to its neighbors when an event occurs. Then, other vehicles assess the sending vehicle's level of trust by verifying the event message in the mining phase. In fact, they use message-checking properties [8] to confirm the reliability of the message. Moreover, with this work, the authors aim to prove that applying blockchain technology in a vehicular environment can ensure the authenticity of the broadcast messages, as well as, guarantee the anonymity requirement. However, this solution suffers from a high computational delay during the block generation phase caused by the use of the PoW consensus.

The architectures in [78], [79], and [8], use vehicles as blockchain nodes for consensus mining and block creation. This can be an advantage for vehicles to have access to the data shared in the blockchain, however, this large number of validators can negatively impact the performance of the network by slowing down the blockchain process. Actually, researchers have mentioned in [80], that as the number of blockchain nodes increases, the time to reach a consensus also increases. Moreover, as vehicles are characterized by limited storage resources compared to RSUs, they may have storage overhead problems. Therefore, several recent solutions, as in [81], have proposed to use RSUs as blockchain nodes to store the blocks.

Yang et al. [81] have suggested a blockchain-based system to manage trust among network nodes by storing vehicle trust levels in distributed ledgers. In this system, the validation of the trustworthiness of received messages is supported by the Bayesian inference model. Next, each message sender is evaluated based on the validation results already done. Then, the RSUs compute vehicles' trust level offsets using the evaluations received from vehicles and collect this data in a block. Finally, each new block is broadcast to all RSUs in the blockchain network to be validated and added to the distributed ledgers. In particular, the authors in this work used a combination of PoW and PoS consensus to validate the trustworthiness of messages. However, this solution has problems with privacy preservation. In fact, the use of the real identity of the vehicle makes it easy to track it and find its owner. Moreover, this solution employs RSUs as miners. However, as Kang et al. [82] point out, RSUs are located all over the road and lack adequate protection. Therefore, they cannot be fully trusted and can lead to serious security/privacy problems.

The authors of [83] pointed out that for fast, secure and efficient data exchange between intelligent vehicles, a more trustworthy network is needed. For this reason, the authors chose to use blockchain technology based on rewards in order to implement *TrustBit*, which is a system that secures communication between intelligent vehicles. In this system, each vehicle in the network has a unique cryptographic identifier, called Intelligent Vehicle Trust Point (IVTP), used to maintain trust in the network. IVTP works like a crypto-currency. If a vehicle has more IVTPs, it will be more trusted and have more points. The IVTP ensures quick and secure communication between vehicles. It also provides access to vehicles' track record from the blockchain. Moreover, the authors of TrustBit used a method called the proof of driving to check and validate vehicles participating in VANET communication. Nevertheless, they don't explain the principle of the proof of driving and why it will be an effective method for reaching a consensus. Moreover, they did not give details on how this system will be realized. Besides, there will be no control over the data of a vehicle if it has lost its IVTP-ID.

Summary In this subsection, we summarize solutions that employ blockchain to store entities or messages' reputations, as presented in Table 6. Indeed, instead of using the blockchain to record and share basic safety information, the authors of these solutions record and share vehicle reputation scores on the blocks. To ensure trustworthiness, some solutions [78], [81], [83] employed blockchain to record vehicles reputations. As far as, these reputation scores will be required by other entities to authenticate or assess the sender's credibility. On the other hand, authors in [79] have used blockchain technology to develop a reputation solution and assess data credibility. In fact, received messages are evaluated according to traffic network observations. Then, these evaluations are grouped in a block. A third use case of blockchain for reputation in the vehicular network was presented in [8]. In this case, the blockchain was applied to store messages and node trustworthiness in the distributed ledger that will be used by other vehicles as proof of truth.

5.3. Privacy preservation

With the increasing development of computer and sensor capabilities embedded in vehicles, the collection and provision of data from vehicles have become very significant for C-ITS to work efficiently and economically. However, gathering and supplying data for C-ITS involves exposing the privacy of vehicles and their drivers, which makes them vulnerable to security threats. Therefore, data linked to the privacy of users (i.e., location, activities, car model) can be traced. Some services that are provided by C-ITS, such as smart parking and car/ride sharing may also greatly expose users' privacy while bringing convenience to users. While no fundamental measures have been taken to protect users' privacy, certain blockchain-based solutions have been proposed to handle this challenge.

As blockchain has become a hot platform to achieve some security properties, some secure parking systems are designed atop a blockchain. Amiri et al. have defined in [84] a blockchain-assisted privacy-preserving smart parking system, where users can retrieve the parking offers nearby without leaking privacy through a method named Private Information Retrieval (PIR). This scheme aims to help drivers to search for and book parking spaces in advance while preserving their privacy. In this system, the blockchain consortium is maintained by forming the parking lot owners together. In fact, they share their parking offers with other information. Then, these offers will be stored on the ledgers of the blockchain. The authors also used the PIR technique in order to preserve the privacy of the location of the vehicle drivers. Indeed, the PIR technique allows drivers to inquire about available parking spaces without revealing their destinations. When a parking offer has been retrieved, the driver applies a randomizable short signature to directly confirm the reservation with the owner of the parking without using the real identity. Therefore, drivers are able to pay in an anonymous way instead of using traditional payment card systems that might reveal confidential information.

Table 6
Comparison of Reputation solutions.

References	Applications	BC Function	BC Type	BC Technology	Consensus	BC Participants	Smart Contract	Evaluation	
								Simulation/ Experimentation	Metrics
[78]	Action selection strategy (choose a reliable relay OBU)	Trust, Transparency	N/A	N/A	N/A	Vehicles		Simulation	- Performance of the action selection strategies
[79]	Data credibility	Transparency, Immutability	N/A	N/A	N/A	Vehicles		Simulation	- Message detection accuracy
[8]	Traffic management	Immutability, Transparency	Public	N/A	PoW	Vehicles	X	Simulation	- Storage and message overhead
[81]	Message credibility	Trust, Immutability	N/A	N/A	PoW + PoS	RSU		Simulation	- Offset block generation time - Messages and ratings transmission latency - Trust value offsets calculation
[83]	Traffic deadlocks	Trust, Immutability	N/A	N/A	PoD	Vehicles		N/A	N/A

Another service in which blockchain technology has also been integrated is the carpooling service. In order to reduce jams, driving time, and environmental pollution, drivers can exchange their destinations in a shared platform to meet passengers with a common travel route. Therefore, by incorporating blockchain technology, several users can share the same vehicle while guaranteeing privacy. Li et al. [85] combined blockchain technology and fog computing to propose a new carpooling scheme called "eFficient prIvacy-preserving CArpooling system (FICA)". To ensure users' privacy and security, the authors proposed to apply digital signatures based on asymmetric keys. In addition, to authenticate the system users and retrieve malicious users' real identities, they implemented an anonymous authentication scheme. Besides, they mentioned that they have adopted the PoS consensus algorithm to enforce the integrity of the carpooling information recorded in the blockchain. Blockchain technology is deployed at the RSU (fog node). The blocks are composed of the carpooling services (transactions) and the stake distribution. The number of carpooling records processed by each RSU presents its stake. Then, upon a proportional probability of the stakes, a leader for each block will be selected. Furthermore, to address cloud computing limitations such as query and reply delays and additional communication overhead, the authors proposed to use fog nodes in their solution. Fog computing offers low latency due to local data processing. In particular, to ensure data reliability and traceability, they encrypted the carpooling data and stored the hash value on the private blockchain, although the details are stored on the cloud. However, they did not study the case where RSUs are attacked. Furthermore, they stated that the cloud server and RSUs are semi-confident. Thus, if the server fails or the data is altered, the system will not be able to verify trustworthiness.

Another similar service in which the blockchain is embedded is the Ride Hailing Services (RHS). Li et al. [86] have employed blockchain technology with vehicular fog computing to implement a Collaborative Ride-hailing service (CoRide) that maintains user privacy. The authors have eliminated the requirement for an online trust authority and they have replaced it with an aggregation of multiple Service Providers (SPs) working together. In fact, they built an immutable consortium blockchain among the SPs to store transactions and execute smart contracts automatically applied on RSUs (fog nodes) to connect drivers with riders. To improve the security of their solution, Li et al. reused three techniques already proposed in the literature [87][88][89]. First, to build secret keys for both user correspondence and trading and to authenticate the locations of users, the authors of CoRide leveraged the private proximity test [87]. Second, to handle pilot filtering and target mapping, they used the privacy-preserving query processing technique presented in [88]. Finally, to perform anonymous payment between all users and detect double-spending threats, Li et al. integrated a modified version of the Zerocash technique [89]. Nevertheless, the SPs and the RSUs are semi-honest and like the previous solution, the case when the RSU is being compromised by adversaries or colluding with SPs is not considered.

Another significant use case for C-ITS is the support of traffic control. Since vehicle operators or detectors are susceptible to sense road nuances, it is becoming easier to collect vehicular traffic information from vehicles. However, a major issue in vehicular communication and traffic exchange is the confidentiality preservation of the vehicle's private information. In order to preserve the privacy of vehicle information, researchers in [90] implement a semi-centralized system using an attribute-based blockchain. In addition, to improve traffic flow, the authors used a control method to manage traffic light signals. Next, before the communication starts, participants must be grouped by their attributes (e.g., positions and directions). Then, participants reach an agreement on a temporary signaling time by interoperating among themselves while ensuring confidentiality and privacy. Finally, they store the agreement and the final decision in the blockchain ledger. Moreover, to maintain privacy between vehicles, the authors propose to use anonymous vehicular communication. The proposal not only meets the goal of preserving privacy but also supports liability investigation for legacy deals using Ciphertext-Policy Attribute-Based Encryption (CP-ABE).

In another work [91], researchers also referred to authentication privacy preservation as the main problem in VANET threat protection. They highlighted that the centralized Trusted Authority (TA)-based solution has two major drawbacks. First, operations are not transparent, which poses security threats. Second, a receiver needs to look up a CRL for message authentication, which results in a high computational load. To address these issues, authors of [91] develop a VANET system that preserves authentication privacy using blockchain technology, the proposed system is named "Blockchain-based Privacy-Preserving Authentication (BPPA)". In addition, to ensure transparency and auditability of semi-trusted authority operations, transactions and all users' certificates are saved immutably and persistently in the blocks of the blockchain. Besides, more than one certificate has been used by vehicles, in order to guarantee conditional privacy. The correspon-

Table 7
Comparison of Privacy Preservation solutions.

References	Applications	BC Function	BC Type	BC Technology	Consensus	BC Participants	Smart Contract	Evaluation	
								Simulation/ Experimentation	Metrics
[84]	Smart parking	Anonymity, Transparency	Consortium	Quorum	Raft	Parking lot Owners, Drivers		Experimentation	- Communication overhead
[85]	Carpooling	Auditability, Traceability	Private	N/A	PoS	RSUs (Fog nodes)		Simulation	-Computational cost - Communication overhead
[86]	Ride Hailing	Disintermediation	Consortium	Ethereum	PoS	RSUs (Fog nodes), Service Providers	X	Experimentation	- Computational cost - Communication overhead
[90]	Traffic management	Transparency, Anonymity	Private	Own Blockchain	Own consensus	Drivers, Infrastructures, (e.g., traffic signal controllers)		Experimentation	- Time consumption for each phase in SCTSC model - Time consumption in CP-ABE encryption
[91]	Anonymous authentication	Transparency, Immutability	Consortium	Hyperledger Fabric	Proof of Presence (PoP)	Law Enforcement Authority, RSUs, Vehicles		Experimentation	- Cost and latency of issuing and revoking certificates - The overhead of the authentication process
[92]	Traffic management	Traceability, Immutability	Private	Bitcoin	Own consensus	Trace managers, RSUs, Vehicles		Simulation	- The average of computation time - The average of communication time

dence between these certificates and the real ID is encoded and then saved in the blockchain. To evaluate the performance of their system the authors used the Hyperledger Fabric technology and compared it with the baseline approaches.
In [92], Li et al. presented a privacy-preserving blockchain-based solution, called *CreditCoin*. CreditCoin is able to build trust in communications of smart vehicles and to maintain the reliability of vehicles' announcements without revealing users' privacy. The privacy of participants generating the announcements is protected by the threshold ring signature scheme. The threshold ring signatures provide indistinguishability among all ring members, but only a part of the members are the actual signers of the signature. This means the group of participants of the announcements will be concealed in a larger group of possible signers. Specifically, if the verification succeeds, the verifier would know that this announcement is valid. The verifier also knows that over N participants claim the correctness of the announcement with a ring signature. However, he does not know the identities of the participants. In CreditCoin, the authors design their own consensus based on the Byzantine Fault Tolerates (BFT) algorithm. RSUs and official public vehicles undertake the work of consensus and make use of the proposed BFT-based mechanism, which repeats a voting process until an agreement is reached. The main drawback of the CrediCoin proposal is the limited scalability, which is inherited from the use of a BFT-based consensus.

Summary Blockchain technology has improved data security and privacy by encrypting and storing data on a decentralized system. Different applications including Smart parking [84], Carpooling [85], Ride-Hailing [86], Traffic management [90,92], and Anonymous authentication [91] are based on blockchain technology to preserve data and entities privacy. As presented in Table 7 all the proposed solutions used a permissioned blockchain whether private or consortium. The permissionless blockchain is characterized by a higher transparency than the permissioned blockchain, which makes it more susceptible to privacy attacks. In fact, the access controls used with permissioned blockchain allow them to be more resistant to privacy attacks. Therefore, it is recommended to use permissioned blockchain for a certain type of application where transactions may include delicate information like users' location, such as carpooling and ride-sharing. This is due to the fact that a hacker can trace a user's transactions via their address and analyze them to deduce their real identity. Therefore, users' wallets or accounts can be compromised, and the malicious actor could do as he or she pleases with the compromised wallet and account. Furthermore, depending on the blockchain technology used for each solution, different consensus mechanisms are employed. A number of these proposals focus on using and enhancing existing blockchain technologies. While others seek to develop new blockchain technologies and new consensus that meet vehicular environment constraints. Finally, we remark that some solutions are only at the simulation stage and the evaluation of their feasibility is not yet performed.

5.4. Data sharing

More and more vehicles are fitted with sensors that monitor the vehicle's condition and surrounding road users. With the right information arriving in the right place at the right time, a transport system can run more smoothly, and smoother operations can lead to safer operations. While most of this sensor data currently remains localized within the vehicle, it could be shared to improve vehicle services. Therefore, data sharing between stakeholders can be the future of transport systems. Besides, sharing data between traffic infrastructure and connected vehicles, for instance, can enhance both traffic efficiency and road safety by delivering critical, just-in-time information.

Undoubtedly, choosing suitable technology and infrastructure is a key factor for efficient data sharing in terms of security and trustworthiness. In this direction, blockchain technology could be a

good candidate for immutable, secure, and transparent data sharing in several C-ITS applications.

The remainder of this section provides a literature review of recent blockchain-based data sharing solutions mainly in four C-ITS applications: (i) forensic services, (ii) vehicles life-cycle, (iii) insurance fraud, and (iv) traffic deadlocks

In the first use case, information collected from both within and around vehicles can significantly impact **forensic services**, which focus on investigating the origins of accidents. With the spread of self-driving cars, data gathering will become increasingly critical, as these vehicles are susceptible to malfunctions and cyberattacks [93]. In general, after an accident, the investigators require certain information, namely the examination of the accident scene and the vehicle status, to analyze the causes of the accident and to resolve the litigation between the concerned parts. Applying blockchain technologies in digital forensics, allows the examiner to perform self-verification for digital evidence.

In this context, Cebe et al. [94] employ blockchain technology in a vehicular system to implement a forensic model that brings vehicles and associated business components under one roof. The use of blockchain technology in this system ensures trust between the different stakeholders of the system namely drivers, car manufacturers, law enforcement, and service centers. The proposed system presents a vehicle forensics framework that hosts all the necessary data for a complete forensics proposal. To solve the problems associated with storage overload, they design a fragmented ledger in which they will store vehicle-related data such as maintenance history, diagnostic reports, etc. Moreover, in order to ensure membership establishment and confidentiality, they proposed to adopt the Vehicular Public Key Management (VPKI) model. In addition, the application of pseudonyms for identities further contributes to user privacy.

In a similar work, the authors in [95] implemented a permissioned blockchain to record connected vehicle activities and interactions. The proposed model is dedicated to auto insurance claims and adjudication services. This model is divided into two partitions. The operational partition which records the vehicle events and the decisional partition which is dedicated to liability decision-making. Therefore, the first partition was controlled and managed by various stakeholders, namely, the Connected and Automated Vehicles (CAV), the car manufacturers, the insurance companies, the software providers, and the service technicians, in order to ensure data transparency between the participants and to prevent any data modification. The second partition was dedicated to the examination of the operational partition available evidence and to the liability decision-making. This partition is managed and controlled by the government transport authorities, the insurance companies, and car manufacturers as well as judicial authorities. Indeed, the major advantage of this separation is that the information is revealed to the concerned parties. However, in their proposal, the authors fail to explain how the proposed consensus operates and why they didn't use the traditional consensus.

For the second data sharing use case, namely **vehicles life-cycle**, new proposals have been recently launched to digitize and secure vehicle odometer readings using blockchain technology. In fact, in the current used car market, the primary reason for devaluation is the lack of trust. One of the most important requirements when selling a used vehicle is the authenticity of the service history, i.e. the vehicle. Although digital counters are included in modern vehicles, fraudulent mileage affects 30% of European used vehicles today, which approximately costs 5.6 to 9.6 billion Euros annually to European consumers [96]. In order to digitize vehicle lifecycles, Brousmiche et al. [97] proposed to employ blockchain technology and to use smart contracts to define secure vehicles' smart service books. The proposed system used a consortium blockchain model to supply a transparent collaboration between different stakeholders, namely, the automotive manufacturer, the insurance company, the vehicle owners, the vehicle retailer, and the maintainers. Vehicle-related data including mileage, maintenance record, sales record, and insurance details are recorded in the form of a certified service book in the blockchain records. In addition, any change in the vehicle's condition, such as in case of an accident, all information will be stored in the blockchain. Therefore, when selling a vehicle, the buyer can have a complete history of the vehicle. The authors suggested using hybrid storage where the consortium ledgers in the cloud servers record only base data, while other types of data (member-specific business information) are recorded locally. Moreover, the author tackled the confidentiality problem related to shared data in the blockchain. They have proposed a novel protocol that enables the sharing of ciphered data and cryptographic keys over the Blockchain. However, the implementation details of the solution are not presented in the paper.

The third use case for blockchain in data sharing applications is **vehicle insurance fraud avoidance**. Such fraud involves misleading an insurance company regarding a claim involving a personal or commercial motor vehicle. Blockchain can detect fraud by allowing real-time information sharing and updating the registry after the agreement of all parties. As an example, Roriz et al. [98] presented a solution based on blockchain to prove the potential of this upcoming technology for insurance fraud prevention. The objective of this proposal is to prevent a particular type of double-dip fraud, where a vehicle is underwriting with multiple insurance companies. Thus, if an accident occurs, the vehicle may collect money from different companies. In order to address the risk of double-dipping insurance fraud, before creating new insurance coverage, companies consult blockchain ledgers to check whether the actual vehicle is engaged in other insurance policies. This system also enables insurers to easily check the vehicles' insurance history. However, the proposed solution is still in the prototype phase.

Finally, blockchain-based data sharing has been recently proposed in the **traffic deadlocks** use case. In this context, Autonomous Vehicles (Autonomous Vehicles (AV)) negotiate the right of way before crossing each intersection without traffic lights, as the vehicle entering the corner first has the right of way. If four AVs arrive at a four-lane crossing almost simultaneously, none of them can move forward until the right of way has been determined, resulting in deadlock in traffic signal-free intersections. Actually, the use of a cooperative traffic management system allows road intersection control, which subsequently improves traffic performance. However, this may not always be feasible because most of the traffic signal-free intersections are located in low-traffic areas. In addition, the deployment of this type of system can result in high maintenance costs.

To solve the mentioned problem, authors of [99] implemented a blockchain-based model that aims to manage intersection traffic while guaranteeing communication security and data integrity of Intelligent Vehicles (IVs). Whenever a vehicle broadcasts a message, the broadcast message should be validated and a PoW is executed. In this system, vehicles are not required to wait longer for their message validation. Intelligent Vehicle Trust Point (IVTP) [83] is employed to verify trustworthiness of a vehicle. Fig. 8 illustrates an example in which four vehicles, namely IV_1, IV_2, IV_3 and IV_4, are coming to an intersection. Vehicles should broadcast their signals as they approach the intersection. Next, a consensus is initiated to determine which vehicle has the oldest time stamp to prioritize and move first. Then, a similar process is used for the next three (or more) vehicles. In our example, Fig. 8, we consider that vehicles IV_1, IV_2, IV_3, and IV_4 arrive to the intersection at time 10:06, 10:02, 10:04 and 10:03, respectively. Once consensus is reached, the network member agrees that IV-2 has the priority to cross the intersection first.

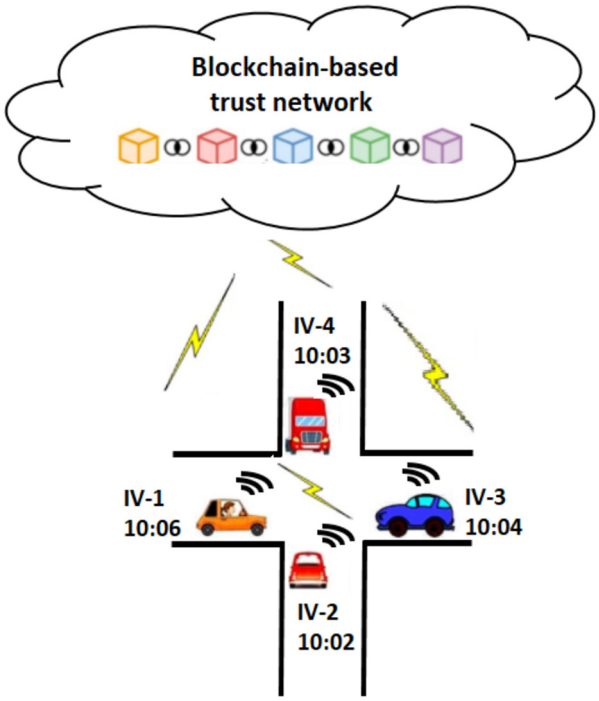


Fig. 8. Example of deadlock at traffic signal-free intersections (first come, first served) for AVs.

However, this type of application can cause storage problems in the blockchain ledgers, especially storage for a long period of time. To tackle these issues authors in [100] propose a branch-based blockchain solution for intelligent vehicles. They incorporate multiple parallel blockchains to speed up the validation time of messages. In addition, their architecture aims to reduce the time consumption of the block mining process. The main entities in this system are as follows: local and global blockchain, intelligent vehicle trust point [83], and branching and unbranching mechanisms. Local blockchain temporarily stores the data and keeps on removing the old data from time to time whereas the main blockchain stores all the transactions between two vehicles permanently. Branching and unbranching mechanisms are used when a block has to be appended to the blockchain. The system's shortcoming is that employing a circular queue led to significant data loss because there was no control and balance over the block that should be replaced by the new block.

Summary Given its key features, namely decentralized data storage, immutability, and transparency, blockchain technology can be a good candidate to replace conventional data sharing solutions that follow a centralized architecture. As shown in Table 8, blockchain technology can be applied to share data in several C-ITS applications, like forensic [94,95], vehicles life-cycle [97], insurance fraud [98], traffic deadlocks [99,100]. Moreover, as presented in the table, all the proposals use the blockchain due to its immutability, transparency, and trust. In fact, some use cases require data storage in a tamper-proof manner, because these data can be used to identify the faulty parties in an accident scenario. Furthermore, blockchain has been used to detect fraud by sharing in real-time each new information and authorizing the ledger modification only upon reception of an agreement from all the involved parties. Besides, blockchain technology provides transparency and collaboration among the stakeholders of the system. The participants can collaborate through the blockchain without needing trust or even familiarity with the other party, the use of the blockchain is a sufficient source of truth for them.

6. Comparison & discussion

In this section, we present a comparative analysis of the solutions described in Section 5. As shown in Table 9, this comparison is made according to the criteria that we identified in Section 4. These criteria are used to evaluate the performance of each solution and to define the strengths and weaknesses of each of them.
For each solution we checked whether this criterion is satisfied (+), or not (-), or N/A, and the appropriate symbol is placed in the cell of the matrix. N/A means that it was not clear in the solution whether this criterion is met or not. For example, for the "Mobility" criteria, if vehicles' mobility doesn't impact the operation of the blockchain-based solution then a (+) is recorded, else a (-) is assigned.
Fig. 9 presents the number of criteria satisfied for each solution. The range of solution is those cells that will be tested against the given criteria and counted if the criteria are satisfied. As shown in Fig. 9, no solution meets all the criteria. We notice that at most two solutions can satisfy four criteria at the same time [85,86]. In addition, as illustrated in Fig. 9, there are some solutions that satisfy only one criterion [78,83,90,99], two criteria [71,72,74,73,75,79,81,84], or three criteria [77,8,91,94,95,97,98], there are others that do not meet any criterion [92].
Fig. 10 shows the percentage of solutions that satisfy each criterion. Here we have made the sum of solutions by criterion, that is to say, each criterion is satisfied by how many solutions. Then we calculated the percentage for each of them. We notice that 65% of the proposed solutions address security problems. Moreover, as presented in Fig. 10, 52% and 43% of the proposed solutions address the mobility issues and the communication overhead problems respectively. However, we observe that only 34% and 21% of the proposed solutions elaborate on the storage requirement issues and the latency problems, respectively.

7. Open research issues

As mentioned in Section 5, a variety of blockchain-based vehicular applications have been developed and discussed. A major advantage of this integration is the potential to improve the C-ITS environment. Nevertheless, many important research questions remain to be answered before the widespread implementation of these integrations. In this section, we highlight some open issues regarding blockchain integration in vehicular networks that could become new research areas in the future.

7.1. Privacy

Since blockchain operations cannot be totally anonymous i.e. use pseudonyms, the blockchain could induce privacy problems. Actually, due to the particularity of transparency of the blockchain and especially for the public blockchain, the exchanged data as well as some sensitive information such as the sender and the receiver addresses are visible to everyone on the network. Therefore, users' activities could be traced by analyzing blockchain ledgers data. Subsequently, by applying certain functions to this data, it becomes very easy to reveal the user's true identity. Then, after determining his or her true identity, all of that user's activities will be tracked and their personal information, such as the vehicle location, will be disclosed. Therefore, it is very important to guarantee true anonymity. Moreover, all sensitive information should stay private. Therefore, access management is required, to control participants.

7.2. Scalability

Deploying blockchain technology in a vehicular system may lead to a scalability challenge, especially if we aim to implement

Table 8
Comparison of Data Sharing solutions.

References	Applications	BC Function	BC Type	BC Technology	Consensus	BC Participants	Smart Contract	Evaluation	
								Simulation/ Experimentation	Metrics
[94]	Forensic	Transparency, Immutability, Trust	Permissioned	N/A	PBFT	Drivers, Manufacturer, Insurance companies, Law enforcement, Maintenance centers		N/A	N/A
[95]	Forensic	Transparency, Immutability, Trust	Permissioned	N/A	Own consensus	CAV, Insurance companies, Auto Manufacturer, Legal authorities Government transport authorities, service technician		Simulation	- Average validation time for each BC partition - B-FICA Overhead evaluation
[97]	Vehicles life-cycle	Immutability, Transparency, Trust	Consortium	Quorum	Quorum	Manufacturer, Insurance companies, Provider of document (i.e. invoices, certificates)	X	N/A	N/A
[98]	Insurance fraud	Immutability, Transparency, Trust	N/A	Ethereum	N/A	Vehicle, Insurance companies	X	N/A	N/A
[99]	Traffic Deadlocks	Trust, Immutability, Transparency	N/A	N/A	PoW	Vehicles		N/A	N/A
[100]	Traffic Deadlocks	Trust, Immutability, Transparency	N/A	N/A	PoW	Vehicles		Experimentation	- Average verification time for a state change

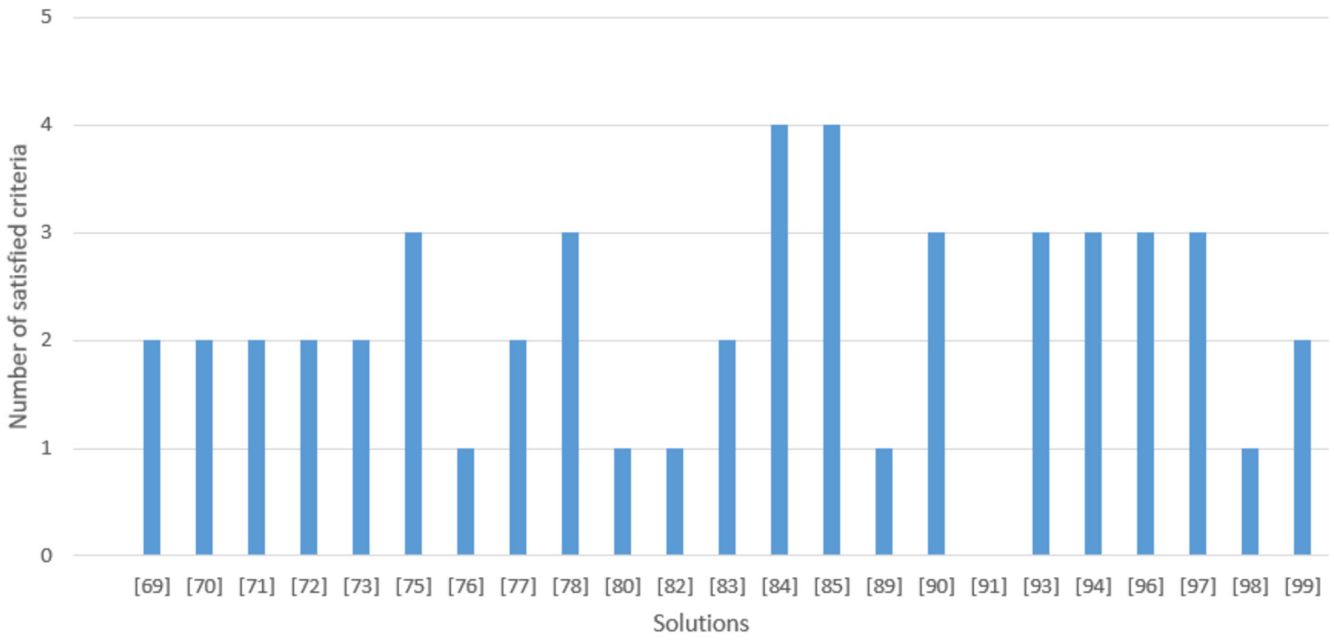


Fig. 9. Number of satisfied criteria per solution.

Table 9
Solutions evaluation according to different criteria.

Reference	Year	Major contribution	Criteria				
			Mobility	Latency	Storage	Overhead	Security
[71]	2019	Developed a decentralized blockchain-based ride-sharing architecture to ensure trust between different entities in the network	-	-	-	+	+
[72]	2018	Suggested blockchain-based VANET scheme for vehicle authentication and revocation	+	-	N/A	N/A	+
[73]	2019	Proposed a CLPKS model to preserve V2I communication privacy using bilinear matching-based conditional authentication	+	-	N/A	+	N/A
[74]	2019	Introduced a blockchain-based authentication model for secure access between vehicles and roadside units	+	-	+	-	-
[75]	2018	Developed a lightweight blockchain-based authentication method to track the status of vehicles certificate	+	-	-	+	-
[77]	2017	Proposed the elimination of central key manager and use of blockchain technology to dynamically manage the keys of a heterogeneous ITS network	+	-	+	-	+
[78]	2018	Implemented a reputation model based on indirect reciprocity. The blockchain technology was used to guarantee the integrity of reputation data	-	N/A	-	N/A	+
[79]	2017	Introduced a blockchain scheme that assures data credibility using vehicle reputations	-	-	-	+	+
[8]	2019	Proposed a blockchain system that stores node and message trustworthiness at the same time to ensure more secure data exchange in VANET	-	-	+	+	+
[81]	2019	Implemented a blockchain-based VANET system that uses the Bayesian inference model to manage trust between network entities	+	-	-	+	-
[83]	2017	Introduced blockchain-based intelligent vehicle communication using rewards. A unique cryptographic id IVTP which is used for maintaining trust in the network	-	-	-	-	+
[84]	2019	Suggested a blockchain-based smart parking system that aims to protect the privacy of participants	-	N/A	-	+	+
[85]	2018	Proposed a carpooling system based on fog computing that uses blockchain technology to preserve the entities' privacy	+	+	+	+	-
[86]	2019	Suggested a Collaborative-Ride hailing system that preserves entity privacy using blockchain technology and vehicular fog computing paradigm	+	+	+	+	-
[90]	2019	Developed a semi-centralized VANET model to balance the tradeoff between privacy preservation and availability using blockchain technology	-	N/A	N/A	N/A	+
[91]	2019	Introduced a BPPA scheme aims to preserve vehicles' identity by storing vehicular data and certificates in the blockchain ledgers	+	+	-	+	-
[92]	2018	Suggested a Blockchain-based vehicular announcement model, which allows vehicles to share network data including traffic status while preserving their privacy	-	-	N/A	-	-
[94]	2018	Proposed a blockchain-based automotive forensics solution that collects pertinent information from various stakeholders in the event of an accident	+	+	N/A	-	+
[95]	2018	Introduced a blockchain-based vehicular auto insurance claims and adjudication system to preserve the integrity of evidence data in the network	+	+	N/A	-	+
[97]	2018	Presented a framework for digitizing the vehicle life-cycles using the consortium blockchain	+	N/A	+	N/A	+
[98]	2019	Discussed how the use of blockchain technology and smart contracts in auto insurance could avoid the fraud issues of the vehicular insurance systems	+	N/A	+	-	+
[99]	2018	Proposed a blockchain system which ensures the integrity of data and secure communication between different vehicles.	-	-	-	-	+
[100]	2018	Proposed a branch-based blockchain model for intelligent vehicle systems	-	-	+	-	+

and operate a large-scale system. As C-ITS environments become larger, new sensors and devices are continuously integrated. The seamless integration of the increasing number of sensors and platforms will pose a real scalability issue. Moreover, to evaluate the scalability of a blockchain network, we consider the rate of transactions per second versus the number of nodes in a network. Currently, existing blockchain platforms are unable to meet the requirements of a vehicular network as these platforms are characterized by low processing throughput, i.e. 7 and 20 transactions per second respectively for Bitcoin and Ethereum. However, the vehicular system processes a large amount of data per second. In addition, various C-ITS applications operate primarily with real-time data. Thus, these applications will face many difficulties to operate effectively due to the limited throughput of the blockchain. Therefore, it is necessary to continue research to find an effective solution to this problem.

7.3. Interoperability

Owing to the variety of formats of the data exchanged in the vehicular network, establishing an interoperable blockchain system is a challenging task. This complication is further compounded

Fig. 10. Percentage of solutions that satisfy each criteria.

because of the different consensus algorithms employed in the systems. MOBI[5] It launches the first Vehicle Identification (VID) standard by integrating blockchain technology into a digital vehicle identification system. MOBI drives adoption, enables interchange and interoperability, and reduces the risk for both integrators and users. Standardization of blockchain technology is expected to align with existing international vehicular industry standards. Therefore, the standardization of a blockchain-based C-ITS system is of great concern and requires further investigation.

7.4. Consensus

Current blockchain technologies and consensus mechanisms present a problem with energy consumption. As previously explained, the PoW consensus requires high computational power and energy consumption. Hence, researchers have worked on the definition of alternative consensus mechanisms that are less computationally expensive for blockchain networks, including PoS and DPoS. However, these mechanisms need further improvements since they can confront security problems. Therefore, it is interesting to think of improving existing consensuses or implementing new ones that meet the requirements of the vehicular network.

7.5. Connectivity

Vehicular networks are characterized by irregular and relatively weak connectivity. This is due to the speed of nodes (vehicles), their random movements, and their behavior in the face of obstacles, which thus makes the connectivity duration between the nodes very short. In addition, connectivity between participants can affect the performance of the blockchain. Indeed, the failure of communication during consensus induces a longer consensus time [102], which directly impacts the network latency. Moreover, communications issues can cause problems in the blockchain process namely the fork situation, i.e. when the node that is eligible to validate a block is not the first who sends the verification information to other participants.

Therefore, nodes with high connectivity capacity may have an inequitable opportunity for mining rewards. Hence, it is necessary to perform a generalized and rigorous analysis of certain parameters such as connectivity to study their impacts on the performance of the blockchain-based vehicular network.

7.6. Security

The major attacks that threaten blockchain technology are the 51% attack, the Denial-of-Service (DoS) attack, and the quantum attack. Actually, in a blockchain the validation of a block is based on a majority vote, i.e., for example with PoW the winner will always be the branch with the most powerful workers behind it. Therefore, if the 51% of the processing resources are under the control of a single entity, the latter can be attacked. Subsequently, the blockchain will be attacked and controlled by a malicious node. After controlling the blockchain, the attacker can conduct double-spending attacks.

During a denial-of-service (DoS) attack, a hacker tries to damage a service's operations or render it completely non-functional. Indeed, DoS attacks typically target network bottlenecks or single points of failure. The decentralized architecture of blockchain technology makes it less vulnerable to the single points of failure issue, however, this type of attack can still exist. Therefore, the execution of the DoS attack depends on the blockchain's technology and where the single points of failure and the bottlenecks occur within the blockchain operation.

Finally, the advent of quantum computing could really threaten the security of the cryptographic hashing techniques on which the whole blockchain philosophy relies. Therefore, the security of the blockchain against vulnerabilities and attacks is of great concern and requires further investigation.

Proposing a blockchain-based security framework to improve the security of C-ITS applications and address all the challenges discussed remains a significant scientific and technical challenge. However, integrating the Mobile Edge Computing (MEC) model into the blockchain-based C-ITS architecture can bring numerous benefits and resolve most of the previously discussed issues.

- Decentralization: MEC enables decentralized data processing and storage, aligning with the decentralized nature of blockchain technology and enhancing the security and reliability of data transfer.
- Data security: MEC enables secure data processing at the edge, which can enhance the security of sensitive data transmitted on the blockchain.
- Reducing latency: MEC reduces latency by processing data more quickly at the source, which can enhance the real-time performance of C-ITS applications using blockchain technology.
- Scalability: MEC can provide the necessary computing resources required for the growth of blockchain-based C-ITS applications and for managing the increased amount of data produced by connected and autonomous vehicles.
- Cost savings: By reducing the amount of data that must be transferred to central servers, MEC can reduce the cost of data processing, making blockchain-based C-ITS systems more cost-effective.

Overall, the integration of MEC into the C-ITS architecture of the blockchain can enhance the performance, security, and efficiency of the system.

8. Conclusion

The continuing advancement and improvement of C-ITS have attracted considerable interest from academic and industrial communities. C-ITS contribute greatly to improving road safety, enhancing traffic flow, and providing in-vehicle entertainment services. Blockchain is a decentralized technology that aims to use the cryptography mechanism to securely store and share system data.

In this paper, we present a comprehensive review of the opportunities and merits of blockchain-based C-ITS applications, as well as their compromises. The study starts with a few recently published investigations and a basic understanding of blockchain technology. Next, we presented the motivation around the integration of

[5] The Mobility Open Blockchain Initiative [101] is a new consortium, composed of leading automotive and technology companies, to create blockchain solutions for the automotive industry.

blockchain into the vehicular environment. Indeed, we explain how blockchain features such as trust, immutability, transparency, and availability provide great potential for solving different problems in current vehicular systems.

The paper has highlighted the major challenges of blockchain-based C-ITS applications. Particularly, mobility, latency, storage requirement, communication overhead, and security. Moreover, we defined a new classification of blockchain-based applications in vehicular networks. We identified 4 categories, namely, identity and access management, reputation, privacy preservation, and data sharing.

Furthermore, our work has presented a qualitative comparison of the discussed solutions according to different criteria. In order to identify the strengths and the weaknesses of each proposal and to figure out the main issues in each architecture related to the integration of the blockchain. The comparison can guide both scientists and practitioners and help them to efficiently develop blockchain-based vehicular systems. Finally, we have specified certain open research issues in blockchain technologies for C-ITS, which can assist researchers to know where they need to focus their future research. We expect that this review will provide a basis for the research and industry communities to move forward.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

No data was used for the research described in the article.

References

[1] R. Ghosh, R. Pragathi, S. Ullas, S. Borra, Intelligent transportation systems: a survey, in: International Conference on Circuits, Controls, and Communications (CCUBE), Bangalore, India, 2017, pp. 160–165.

[2] A. Luckow, K. Kennedy, Data infrastructure for intelligent transportation systems, in: Data Analytics for Intelligent Transportation Systems, 2017, pp. 113–129.

[3] M. Alam, J. Ferreira, J. Fonseca, Introduction to intelligent transportation systems, in: Intelligent Transportation Systems, Springer, Switzerland, 2016, pp. 1–17.

[4] F.J. Martin-Vega, B. Soret, M.C. Aguayo-Torres, I.Z. Kovacs, G. Gomez, Geolocation-based access for vehicular communications: analysis and optimization via stochastic geometry, IEEE Trans. Veh. Technol. 67 (4) (2018) 3069–3084.

[5] H. Guo, X. Zhou, J. Liu, Y. Zhang, Vehicular intelligence in 6G: networking, communications, and computing, Veh. Commun. 33 (2022) 100399.

[6] H. Guo, J. Li, J. Liu, N. Tian, N. Kato, A survey on space-air-ground-sea integrated network security in 6G, IEEE Commun. Surv. Tutor. 24 (1) (2022) 53–87.

[7] H. Guo, J. Liu, J. Ren, Y. Zhang, Intelligent task offloading in vehicular edge computing networks, IEEE Wirel. Commun. 27 (4) (2020) 126–132.

[8] R. Shrestha, R. Bajracharya, A.P. Shrestha, S.Y. Nam, A new-type of blockchain for secure message exchange in VANET, Digit. Commun. Netw. (2019).

[9] D. Puthal, N. Malik, S.P. Mohanty, E. Kougianos, C. Yang, The blockchain as a decentralized security framework, IEEE Consum. Electron. Mag. 7 (2) (2018) 18–21.

[10] J. Xie, H. Tang, T. Huang, F.R. Yu, R. Xie, J. Liu, Y. Liu, A survey of blockchain technology applied to smart cities: research issues and challenges, IEEE Commun. Surveys Tuts. 21 (3) (2019) 2794–2830.

[11] J. Wei, B. Wulan, J. Yan, M. Sun, H. Jing, The adoption of blockchain technologies in data sharing: a state of the art survey, in: Proceedings of the Eighteenth Wuhan International Conference on E-Blockchain (WHICEB), Wuhan, China, 2019, pp. 54–61.

[12] R. Koduri, S. Nandyala, M. Manalikandy, Secure vehicular communication using blockchain technology, in: SAE World Congress Experience, 2020, ISSN: 0148-7191.

[13] P. Fraga-Lamas, T.M. Fernández-Caramés, A review on blockchain technologies for an advanced and cyber-resilient automotive industry, IEEE Access 7 (2019) 17578–17598.

[14] S. Belmannoubi, M. Hadded, H. Touati, F. Kamoun, La Technologie Blockchain pour Améliorer la Sécurité des Systèmes de Transport Intelligents, in: CSTI'20–1er Colloque Francophone des Systèmes de Transports Intelligents, 2020.

[15] F. Wang, Y. Yuan, J. Zhang, R. Qin, M.H. Smith, Blockchainized Internet of minds: a new opportunity for cyber physical social systems, IEEE Trans. Comput. Soc. Syst. 5 (4) (2018) 897–906.

[16] Porsche introduces blockchain to cars [Online], https://www.porsche.com/usa/aboutporsche/pressreleases/pag/?id=479342&pool=international-de&lang=none. (Accessed 15 January 2021).

[17] Toyota Research Institute Explores Blockchain Technology for Development of New Mobility Ecosystem [Online], https://pressroom.toyota.com/toyota-research-institute-explores-blockchain-technology/. (Accessed 15 January 2021).

[18] Groupe Renault, Microsoft et VISEO s'associent pour créer le premier prototype de carnet d'entretien numérique, [Online], https://news.microsoft.com/fr-fr/2017/07/25/groupe-renault-microsoft-viseo-sassocient-creer-premier-prototype-de-carnet-dentretien-numerique/. (Accessed 15 January 2021).

[19] B. Bhushan, A. Khamparia, K. Martin Sagayam, S.K. Sharma, M.A. Ahad, N.C. Debnath, Blockchain for smart cities: a review of architectures, integration trends and future research directions, Sustain. Cities Soc. (2020).

[20] M.A. Ferrag, M. Derdour, M. Mukherjee, A. Derhab, L. Maglaras, H. Janicke, Blockchain technologies for the internet of things: research issues and challenges, IEEE Int. Things J. 6 (2) (2019) 2188–2204.

[21] L. Mendiboure, M.A. Chalouf, F. Krief, Survey on blockchain-based applications in internet of vehicles, Comput. Electr. Eng. 84 (2020).

[22] S. Majumder, A. Mathur, A.Y. Javaid, A study on recent applications of blockchain technology in vehicular adhoc network (VANET), in: National Cyber Summit (NCS) Research Track, 2019, pp. 293–308.

[23] M.B. Mollah, J. Zhao, D. Niyato, Y.L. Guan, C. Yuen, S. Sun, K.Y. Lam, L.H. Koh, Blockchain for the Internet of vehicles towards intelligent transportation systems: a survey, IEEE Int. Things J. (2020) 11.

[24] S. Nakamoto, Bitcoin: a peer-to-peer electronic cash system, 2008, [Online]. Available: https://bitcoin.org/bitcoin.pdf.

[25] S. King, S. Nadal, PPCoin: Peer-to-peer crypto-currency with proof-of-stake, Chainwhy, Tech. Rep., Aug. 2012, [Online]. Available: https://www.chainwhy.com/upload/default/20180619/126a057fef926dc286accb372da46955.pdf.

[26] D. Larimer, Delegated proof-of-stake, Bitshare Whitepaper (2014).

[27] C. Miguel, L. Barbara, Practical Byzantine fault tolerance, in: Proceedings of the Third Symposium on Operating Systems Design and Implementation, vol. 99, New Orleans, USA, 1999, pp. 173–186.

[28] L. Bach, B. Mihaljevic, M. Zagar, Comparative analysis of blockchain consensus algorithms, in: 41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), IEEE, 2018, pp. 1545–1550.

[29] Z. Zheng, S. Xie, H.-N. Dai, X. Chen, H. Wang, Blockchain challenges and opportunities: a survey, Int. J. Web Grid Serv. 14 (4) (2018) 352–375.

[30] D. Schwartz, N. Youngs, A. Britto, The Ripple Protocol Consensus Algorithm, Ripple Labs Inc White Paper 5 (2014).

[31] J. Kwon, Tendermint: Consensus without mining, Draft Version 0.6, 2014.

[32] Proof of Authority, https://github.com/paritytech/parity/wiki/Proof-of-Authority-Chains.

[33] L. Chen, L. Xu, N. Shah, Z. Gao, Y. Lu, W. Shi, On security analysis of proof-of-elapsed-time (PoET), in: International Symposium on Stabilization, Safety, and Security of Distributed Systems, Springer, 2017, pp. 282–297.

[34] J. Kreps, N. Narkhede, J. Rao, Kafka: a distributed messaging system for log processing, in: Proc. NetDB, 2011, pp. 1–7.

[35] D. Ongaro, J. Ousterhout, In search of an understandable consensus algorithm, in: The 2014 USENIX Conference on USENIX Annual Technical Conference, 2014, pp. 305–319.

[36] T.T.A. Dinh, R. Liu, M. Zhang, G. Chen, B.C. Ooi, J. Wang, Untangling blockchain: a data processing view of blockchain systems, IEEE Trans. Knowl. Data Eng. 30 (7) (2018) 1366–1385.

[37] Z. Zheng, S. Xie, H. Dai, X. Chen, H. Wang, An overview of blockchain technology: architecture, consensus, and future trends, in: IEEE International Congress on Big Data (BigData Congress), 2017, pp. 557–564.

[38] Ethereum: Blockchain APP Platforms [Online]. Available: https://www.ethereum.org/. (Accessed 4 November 2020).

[39] Litecoin: an open source P2P digital currency [Online]. Available: https://litecoin.org/. (Accessed 4 November 2020).

[40] MultiChain, Open platform for building blockchains [Online]. Available:, https://www.multichain.com/. (Accessed 4 November 2020).

[41] Hydrachain Project [Online]. Available: https://github.com/HydraChain/hydrachain. (Accessed 4 November 2020).

[42] Hyperledger Fabric Project, [Online]. Available: https://hyperledger-fabric.readthedocs.io/en/release/. (Accessed 4 November 2020).

[43] Corda Project [Online]. Available: https://docs.corda.net. (Accessed 4 November 2020).

[44] R3: Enterprise Blockchain Technology Company [Online]. Available: https://www.r3.com/. (Accessed 4 November 2020).
[45] J. Liu, Z. Liu, A survey on security verification of blockchain smart contracts, IEEE Access 7 (2019) 894–77 904.
[46] D.A. Hahn, A. Munir, V. Behzadan, Security and privacy issues in intelligent transportation systems: classification and challenges, IEEE Intell. Transp. Syst. Mag. (2019).
[47] V. Patil, P.S. Patil, Secured and privacy preserving navigation for VANET, Int. J. Electr. Electron. Res. 3 (2) (2015) 305–309.
[48] F. Jameel, U. Javaid, B. Sikdar, I. Khan, G. Mastorakis, C.X. Mavromoustakis, Optimizing blockchain networks with artificial intelligence: towards efficient and reliable IoT applications, in: Convergence of Artificial Intelligence and the Internet of Things, Springer, New York, NY, USA, 2020, pp. 299–321.
[49] K. Suankaewmanee, D.T. Hoang, D. Niyato, S. Sawadsitang, P. Wang, Z. Han, Performance analysis and application of mobile blockchain, in: Proc. Int. Conf. on Comput., Networking and Commun. (ICNC), Maui, HI, USA, 2018, pp. 642–646.
[50] Z. Xiong, Y. Zhang, D. Niyato, P. Wang, Z. Han, When mobile blockchain meets edge computing, IEEE Commun. Mag. 56 (8) (2018) 33–39.
[51] S. Kim, Impacts of mobility on performance of blockchain in VANET, IEEE Access 7 (2019) 68646–68655.
[52] X. Ma, J. Zhang, X. Yin, K.S. Trivedi, Design and analysis of a robust broadcast scheme for VANET safety-related services, IEEE Trans. Veh. Technol. 61 (1) (2012) 46–61.
[53] B. Hassanabadi, S. Valaee, Reliable periodic safety message broadcasting in VANETs using network coding, IEEE Trans. Wirel. Commun. 13 (3) (2014) 1284–1297.
[54] R. Memon, J. Li, J. Ahmed, M. Nazeer, M. Ismail, Cloud-based vs. blockchain-based IoT: a comparative survey and way forward, in: Frontiers of Information Technology & Electronic Engineering, Springer, 2020.
[55] Q. Zhou, H. Huang, Z. Zheng, J. Bian, Solutions to scalability of blockchain: a survey, IEEE Access 8 (2020) 16440–16455.
[56] A. Gervais, G.O. Karame, K. Wüst, V. Glykantzis, H. Ritzdorf, S. Capkun, On the security and performance of proof of workblockchains, in: Proceedings of the ACM SIGSAC Conference Oncomputer and Communications Security, 2016, pp. 3–16.
[57] X. Wang, X. Zha, W. Ni, R.P. Liu, Y.J. Guo, X. Niu, K. Zheng, Survey on blockchain for internet of things, Comput. Commun. (2019).
[58] Y. Park, C. Sur, H. Kim, K.-H. Rhee, A reliable incentive scheme using bitcoin on cooperative vehicular ad hoc networks, IT Converg. Pract 5 (2017) 34–41.
[59] Y. Park, C. Sur, K.-H. Rhee, A secure incentive scheme for vehicular delay tolerant networks using cryptocurrency, Secur. Commun. Netw. (2018).
[60] S. Hamdan, M. Ayyash, S. Almajali, Edge-computing architectures for internet of things applications: a survey, Sensors 20 (2020) 6441.
[61] Y. Chen, H. Li, K. Li, J. Zhang, An improved P2P file system scheme based on IPFS and blockchain, in: Proc. IEEE Int. Conf. Big Data (Big Data), 2017, pp. 2652–2657.
[62] M. Rehman, Z.A. Khan, M.U. Javed, M.Z. Iftikhar, U. Majeed, I. Bux, N. Javaid, A Blockchain Based Distributed Vehicular Network Architecture for Smart Cities, Web Artificial Intelligence and Network Applications. WAINA, Advances in Intelligent Systems and Computing, vol. 1150, Springer, 2020.
[63] O. Wennergren, M. Vidhall, J. Sörensen, Transparency analysis of distributed file systems: with a focus on interplanetary file system, Tech. Rep, 2018.
[64] H. Huang, J. Lin, B. Zheng, Z. Zheng, J. Bian, When blockchain meets distributed file systems: an overview, challenges, and open issues, IEEE Access (2020) 50574–50586.
[65] H. El-Sayed, M. Chaqfeh, Exploiting mobile edge computing for enhancing vehicular applications in smart cities, Sensors 19 (5) (2019) 1073.
[66] A.M. Souza, G. Maia, L.A. Villas, A data dissemination solution for highly dynamic highway environments, in: Proceedings of the IEEE 13th International Symposium on Network Computing and Applications (NCA), Cambridge, MA, USA, 2014, pp. 17–23.
[67] R. Almadhoun, M. Kadadha, M. Alhemeiri, M. Alshehhi, K. Salah, A user authentication scheme of IoT devices using blockchain-enabled fog nodes, in: IEEE/ACS 15th International Conference on Computer Systems and Applications (AICCSA), 2018, pp. 1–8.
[68] Y. Yao, X. Chang, J. Misc, V.B. Misc, L. Li, BLA: blockchain-assisted lightweight anonymous authentication for distributed vehicular fog services, IEEE Int. Things J. (2019).
[69] R. Iqbal, T.A. Butt, M. Afzaal, K. Salah, Trust management in social internet of vehicles: factors, challenges, blockchain, and fog solutions, Int. J. Distrib. Sens. Netw. (2019).
[70] J. Ni, A. Zhang, X. Lin, X.S. Shen, Security, privacy, and fairness in fog-based vehicular crowdsensing, IEEE Commun. Mag. 55 (6) (2017) 146–152.
[71] R. Shivers, M.A. Rahman, H. Shahriar, Toward a secure and decentralized blockchain-based ride-hailing platform for autonomous vehicles, Ph.D. dissertation, Tennessee Technological University, 2019.
[72] N. Malik, P. Nanda, A. Arora, X. He, D. Puthal, Blockchain based secured identity authentication and expeditious revocation framework for vehicular networks, in: 2018 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications/12th IEEE International Conference on Big, Data Science and Engineering (TrustCom/BigDataSE), New York, NY, USA, 2018, pp. 674–679.
[73] I. Ali, M. Gervais, E. Ahene, F. Li, A blockchain-based certificateless public key signature scheme for vehicle-to-infrastructure communication in VANETs, J. Syst. Archit. 99 (2019).
[74] D. Zheng, C. Jing, R. Guo, S. Gao, L. Wang, A traceable blockchain-based access authentication system with privacy preservation in VANETs, IEEE Access 7 (2019) 117716–117726.
[75] N. Lasla, M. Younis, W. Znaidi, D. Ben Arbia, Efficient distributed admission and revocation using blockchain for cooperative ITS, in: 2018 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS), 2018, pp. 1–5.
[76] S. Rafaeli, D. Hutchison, A survey of key management for secure group communication, ACM Comput. Surv. 35 (3) (2003) 309–329.
[77] A. Lei, H. Cruickshank, Y. Cao, P. Asuquo, C.P.A. Ogah, Z. Sun, Blockchain-based dynamic key management for heterogeneous intelligent transportation systems, IEEE Int. Things J. 4 (6) (2017) 1832–1843.
[78] C. Dai, X. Xiao, Y. Ding, L. Xiao, Y. Tang, S. Zhou, Learning Based Security for VANET with Blockchain, IEEE International Conference on Communication Systems, ICCS, Chengdu, China, 2018.
[79] Z. Yang, K. Zheng, K. Yang, V.C.M. Leung, A blockchain-based reputation system for data credibility assessment in vehicular networks, in: IEEE 28th Annu. Int. Symp. Pers, 2017, pp. 1–5.
[80] S.A. George, A. Jaekel, I. Saini, Secure identity management framework for vehicular ad-hoc network using blockchain, in: IEEE Symposium on Computers and Communications (ISCC), 2020.
[81] Z. Yang, K. Yang, L. Lei, K. Zheng, V.C.M. Leung, Blockchain-based decentralized trust management in vehicular networks, IEEE Int. Things J. 6 (2) (2019) 1495–1505.
[82] J. Kang, R. Yu, X. Huang, M. Wu, S. Maharjan, S. Xie, Y. Zhang, Blockchain for secure and efficient data sharing in vehicular edge computing and networks, IEEE Int. Things J. 6 (3) (2019) 4660–4670.
[83] M. Singh, S. Kim, Introduce reward-based intelligent vehicles communication using blockchain, in: Proc. Int. SoC Design Conf. (ISOCC), 2017, pp. 15–16.
[84] W. Al Amiri, M. Baza, M. Mahmoud, K. Banawan, W. Alasmary, K. Akkaya, Privacy-preserving smart parking system using blockchain and private information retrieval, in: Proc. of the IEEE International Conference on Smart Applications, Communications and Networking, SmartNets, 2019.
[85] L. Meng, L. Zhu, X. Lin, Efficient and privacy-preserving carpooling using blockchain-assisted vehicular fog computing, IEEE Int. Things J. (2018).
[86] M. Li, L. Zhu, X. Lin, CoRide: a privacy-preserving collaborative ride hailing service using blockchain-assisted vehicular fog computing, in: Proc. ACM SecureComm, 2019, pp. 408–422.
[87] Y. Zheng, M. Li, W. Lou, Y.T. Hou, Location based handshake and private proximity test with location tags, IEEE Trans. Dependable Secure Comput. 14 (4) (2017) 406–419.
[88] R. Li, A.X. Liu, Adaptively secure conjunctive query processing over encrypted data for cloud computing, in: IEEE 33rd ICDE, 2017, pp. 697–708.
[89] E. Ben-Sasson, A. Chiesa, C. Garman, M. Green, I. Miers, E. Tromer, M. Virza, Zerocash: decentralized anonymous payments from bitcoin, Proc. IEEE Symp. Secur. Priv. (2014) 459–474.
[90] L. Cheng, J. Liu, G. Xu, Z. Zhang, H. Wang, H.-N. Dai, Y. Wu, W. Wang, SCTSC: a semicentralized traffic signal control mode with attribute-based blockchain in IoVs, IEEE Trans. Comput. Soc. Syst. (2019) 1–10.
[91] Z. Lu, Q. Wang, G. Qu, H. Zhang, Z. Liu, A blockchain-based privacy-preserving authentication scheme for VANETs, IEEE Trans. Very Large Scale Integr. (VLSI) Syst. 27 (12) (2019) 2792–2801.
[92] L. Li, J. Liu, L. Cheng, S. Qiu, W. Wang, X. Zhang, Z. Zhang, Creditcoin: a privacy-preserving blockchain-based incentive announcement network for communications of smart vehicles, IEEE Trans. Intell. Transp. Syst. 19 (7) (2018) 2204–2220.
[93] Z.A. Baig, P. Szewczyk, C. Valli, P. Rabadia, P. Hannay, M. Chernyshev, M. Johnstone, P. Kerai, A. Ibrahim, K. Sansurooah, et al., Future challenges for smart cities: cyber-security and digital forensics, Digit. Investig. 22 (2017) 3–13.
[94] M. Cebe, E. Erdin, K. Akkaya, H. Aksu, S. Uluagac, Block4Forensic: an integrated lightweight blockchain framework for forensics applications of connected vehicles, IEEE Commun. Mag. 56 (10) (2018) 50–57.
[95] C. Oham, R. Jurdak, S.S. Kanhere, A. Dorri, S. Jha, B-FICA: blockchain-based framework for auto-insurance claim and adjudication, in: Proceedings of the IEEE 2018 International Conference on BlockChain, Halifax, 2018, pp. 1171–1180.
[96] T. Willemarck, H. Graafland, C. Gonderinger, J. Cobbaut, B. Lycke, J. Hakkenberg, M. Peelman, Protect European consumers against odometer manipulation, [Online]. Available: goo.gl/CnQuYg, 2014. (Accessed 20 December 2020).
[97] K.L. Brousmiche, T. Heno, C. Poulain, A. Dalmieres, E.B. Hamida, Digitizing, securing and sharing vehicles life-cycle over a consortium blockchain: lessons learned, in: IEEE Int. Conf. New Technol., Mobility Secur., 2018, pp. 1–5.
[98] R. Roriza, J.L. Pereira, Avoiding insurance fraud: a blockchain-based solution for the vehicle sector, Proc. Comput. Sci. 164 (2019) 3–10.

[99] M. Singh, S. Kim, Trust bit: reward-based intelligent vehicle commination using blockchain paper, in: IEEE 4th World Forum on Internet of Things, 2018, pp. 62–67.
[100] M. Singh, S. Kim, Branch based blockchain technology in intelligent vehicle, Comput. Netw. 145 (2018) 219–231.
[101] Mobility Open Blockchain Initiative [Online], https://dlt.mobi/. (Accessed 15 January 2021).
[102] Z. Zheng, J. Pan, L. Cai, Lightweight blockchain consensus protocols for vehicular social networks, IEEE Trans. Veh. Technol. 69 (6) (2020) 5736–5748.