electronics

MDPI

Review

Evolution of V2X Communication and Integration of Blockchain for Security Enhancements

Rakesh Shrestha [1,†], Seung Yeob Nam [2,*,†], Rojeena Bajracharya [3,†] and Shiho Kim [1,*,†]

1 Yonsei Institute of Convergence Technology, Yonsei University, Incheon 21983, Korea; rakez_shre@yonsei.ac.kr
2 Department of Information and Communication Engineering, Yeungnam University, Gyeongsan 38541, Korea
3 Department of Information and Telecommunication Engineering, Incheon National University, Incheon 22012, Korea; rojeena@inu.ac.kr
* Correspondence: synam@ynu.ac.kr (S.Y.N.); shiho@yonsei.ac.kr (S.K.)
† These authors contributed equally to this work.

Received: 20 July 2020; Accepted: 17 August 2020; Published: 19 August 2020

Abstract: With the rapid evolution in wireless communications and autonomous vehicles, intelligent and autonomous vehicles will be launched soon. Vehicle to Everything (V2X) communications provides driving safety, traffic efficiency, and road information in real-time in vehicular networks. V2X has evolved by integrating cellular 5G and New Radio (NR) access technology in V2X communications (i.e., 5G NR V2X); it can fulfill the ever-evolving vehicular application, communication, and service demands of connected vehicles, such as ultra-low latency, ultra-high bandwidth, ultra-high reliability, and security. However, with the increasing number of intelligent and autonomous vehicles and their safety requirements, there is a backlash in deployment and management because of scalability, poor security and less flexibility. Multi-access Edge Computing (MEC) plays a significant role in bringing cloud services closer to vehicular nodes, which reduces the scalability and flexibility issues. In addition, blockchain has evolved as an effective technology enabler to solve several security, privacy, and networking issues faced by the current 5G-based MEC systems in vehicular networks. Blockchain can be integrated as a strong security mechanism for securing and managing 5G V2X along with MEC. In this survey, we discuss, in detail, state-of-the-art V2X, its evolution based on cellular 5G technology and non-cellular 802.11bd. We investigate the integration of blockchain in 5G-based MEC vehicular networks for security, privacy protection, and content caching. We present the issues and challenges in existing edge computing and 5G V2X and, then, we shed some light on future research directions in these integrated and emerging technologies.

Keywords: connected vehicles; security; blockchain; edge computing; privacy

1. Introduction

Vehicles are important part of our daily commute; they have become a necessity rather than a luxury. Vehicle to Everything (V2X) communications provide driving safety, traffic efficiency, and road information in real-time in vehicular networks. The vertical automobile industry is undergoing major technical advances with a revolutionary goal in the development of intelligent and autonomous vehicles. The intelligent and autonomous vehicles may be classified as Automotive Vehicles and Connected Vehicles. The interconnection between vehicles is commonly known as Connected Vehicles in the United States [1] and Cooperative Intelligent Transport Systems (C-ITS) in EU countries [2]. The connected vehicle technology, or C-ITS, is based on VANETs for communicating safety and non-safety messages. Because of the ITS technological advancements, C-ITS has gained a lot of attention from industry and academia

that could potentially help traffic-flow situations (such as congestion, accidents, and road construction), ensure safe driving, and provide multimedia entertainment in vehicles. The advancement of connectivity in vehicles includes different types of communication technologies. In vehicular networks, the vehicle can communicate with neighbor vehicles, infrastructures, pedestrians, cyclists, etc.

After the 3GPP came into the existence with C-V2X technology, they closely focused on its development by launching a range of specification standards to improve the V2X technology further. At the start of the DSRC era, the 3G cellular infrastructure was also in operation; however, it was not able to satisfy the strict specifications needed for V2X communications. Furthermore, with the advancement of wireless technologies, 4G or LTE networks were launched with high speed, low latency, high throughput, and high reliability. LTE for vehicles (LTE-V) was introduced in 2016 as an alternative technology besides DSRC for vehicular networks to support intelligent transportation. However, LTE-V still cannot support ultra-low latency, ultra-high reliability and ultra-high bandwidth requirements for V2X applications, such as critical messages and coordinated platooning. Since then, New Radio (NR) technology has been introduced that enhances the C-V2X applications. Every release has been enhanced further almost every year. The goal of NR V2X is not to replace the already standardized C-V2X technology. The aim is to provide additional support for all V2X applications. In a region where new vehicles will have both C-V2X and NR V2X functionalities, C-V2X and NR V2X will likely coexist. Some of the notable key features of NR V2X are side link mode 2, improved scheduling mechanisms, different transmission mechanisms (like unicast, groupcast, and broadcast), various side link modes, PHY layer improvements, etc. The emerging 5G technology will further help C-V2X and, at the same time, increase security. In contrast to the existing cellular networks, 5G wireless networks will be decentralized and omnipresent, with particular focus on security and privacy requirements. The evolution of C-V2X towards 5G NR V2X provides adequate requirements and new possibilities for current and future intelligent and autonomous driving industries, while, at the same time, retaining backward compatibility.

Meanwhile, edge computing has emerged as an expansion of cloud computing, and it is considered as enabling technology for driving 5G ecosystems forward. It delivers computing facilities at the edge of the network to nearby vehicles or other devices, allowing for even shorter communication delays in processing and storage. In vehicular networks, Multi-access Edge Computing (MEC) reduces delays and background congestion by computation offloading and distributed content caching. It provides a series of computing services such as edge data storage, task processing, real-time network access, and Quality of Service (QoS) improvements with ultra-low latency data transmissions. The decentralized MEC system in vehicular networks offers various advantages, including ubiquitous network connections, increased scalability, and decreased complexity in network operations, and it helps in the development of 5G V2X services. The data computing is vulnerable to malicious attacks in the dynamic edge-computing environment such as jamming attacks, sniffing attacks, denial-of-service attacks (DoS), etc. Furthermore, the edge servers must be reliable and secure, but they can be compromised because of the high dynamicity and accessibility of the MEC-based V2X networks. A further challenge is to protect data privacy and immutability from external modifications or alternations.

The rapid and explosive growth in 5G V2X traffic data generated by high-density vehicles has led to strong demands for network defense systems against various cyber-attacks. Blockchain is expected to offer a range of security services for 5G V2X and edge computing with powerful security properties to enhance overall performance of future V2X networks. Blockchain comes as a suitable candidate to resolve such challenges by securing transactions and verifying the user connections. Blockchain systems provide strong data security by storing data in a distributed ledger, where data are signed and appended immutably to blocks. Blockchain can deliver a wide variety of security advantages, such as access control provided by smart contracts, data integrity, and an efficient consensus verification mechanism. Because of the time-varying channels in V2X, unpredictable network traffic, high-performance protocols and stringent requirements for numerous emerging technologies (edge computing, blockchain and 5G networks) cannot achieve their goal independently. Therefore,

all of the above technologies should be combined, and linked with each other in order to fulfill the essential requirements and functional criteria of the next-generation of vehicular networks.

The 5G-based edge cloud computing provides appropriate services in V2X by collecting, storing, and managing large amount of heterogeneous data. However, new technologies also introduce additional security and privacy issues in integrated 5G and edge based V2X. The outsourcing of huge data to the MEC servers raises serious issues that are linked with the data privacy. Some of the major issues and challenges include data availability, data integrity, data privacy management, confidentiality, heterogeneity, effective wireless resource management, resource scaling, transparency, and immutability. The introduction of blockchain in integrated 5G-based edge computing in vehicular networks provides some advantages, yet, there are issues that are related to scalability and performance based on storage, throughput, incentivem, and network resources. Some of the examples of security flaws in integrated blockchain in 5G-based MEC are time-stamping dependency, mismanaged exceptions, re-entry attacks on smart contracts, and privacy leakage due to the involvement of malicious nodes in the network. All of these issues need to be addressed carefully before implementing 5G networks and edge computing in realistic situations in vehicular networks.

There is research being carried out using blockchain in V2X communication along with 5G-based edge computing networks [3]. By integrating blockchain in 5G-based edge computing in V2X networks, Road Side Units (RSUs), or 5G Radio Access Networks (RANs) can be equipped with MEC storage servers to incorporate MEC and 5G. A fast and effective consensus mechanism is required for efficient block verification to sustain the permissioned blockchain. The integration of the above technologies include a range of services, including convergence, localization, traffic information gathering, traffic data management, communication, and access to the internet services with edge-cloud service layer support. However, there are some gaps that need to be filled for full convergence. When considering these gaps, the primary aim of this paper is to serve as a bridge for researchers who want to design new solutions shifting from conventional VANETs towards integrated V2X networks.

Our systematic literature review on the integration of blockchain into 5G-based edge computing in V2X shows several significant findings that will open up multiple opportunities for newly evolving 5G V2X scenarios. We suggest the integration of blockchain with 5G-based edge computing in V2X that provides efficiency and scalability in vehicular networks. The efficiency can be obtained by having maximum coverage without extra overhead, while scalability can be obtained by maintaining ultra-low latency under various traffic conditions. The key contributions of this survey can be summarized, as follows.

- We survey state-of-the-art V2X technology, including its definition; we highlight the V2X evolution, and provide detailed comparisons of cellular and non-cellular based V2X communication.
- We present a review on the adoption of edge-based computing for V2X communications with particular emphasis on integrating promising technologies, such as MEC and Nonorthogonal multiple access (NOMA), and their applications in data offloading for 5G vehicular networks.
- We investigate the potential of blockchain in V2X networks as a security mechanism. We examine the requirements of V2X and discuss on how the requirements are fulfilled by the blockchain.
- We conducted an in-depth analysis of integrating blockchain with 5G and edge computing in V2X networks, and provide a detailed comparison of the integration of each technology.
- We discuss the open issues and future research directions of integrated V2X networks.

The organization of this paper is as follows. We begin with the introduction in Section 1. Section 2 presents a detailed overview of the V2X technology and discusses state-of-the-art V2X communications. In Section 3, we present the evolution of V2X technology that is based on cellular and non-cellular communications. In Section 4, we provide an in-depth discussion of edge computing for V2X communications, highlighting the integration of MEC and NOMA. Section 5 presents the potential issues and challenges faced by V2X networks. Section 6 provides the detail discussion on the integrating blockchain with 5G and edge computing in V2X networks and includes comparisons. Section 7

discusses the open issues and outline the future research directions. Finally, Section 8 concludes this survey paper. The structure of the survey paper is given in Figure 1.

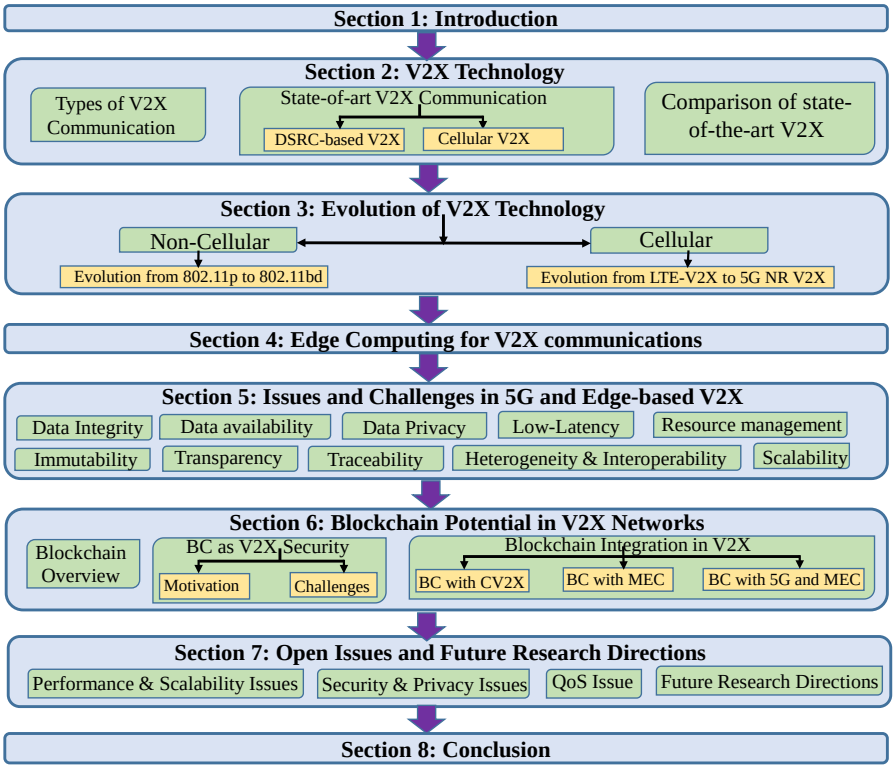


Figure 1. Structure of the survey paper.

2. V2X Technology

According to the 3GPP, the term V2X implies to communication between different entities based on Vehicle-to-Vehicle (V2V), Vehicle-to-Infrastructure (V2I), Vehicle-to-Network (V2N), and Vehicle-to-Pedestrian (V2P) communications, etc. for both safety and non-safety applications [4]. V2X allows vehicular nodes to obtain a wide variety of traffic data in real time that greatly enhances driving security, traffic quality, and infotainment facilities. As the vehicles become more advanced and autonomous, a large number of sensors, and diverse communication devices and technologies will be used, which will generate a huge number of data, such as cooperative sensing data, communications, infotainment, sensing data, etc. The complexity of vehicular applications will further increase, as the density of the vehicles increase and existing V2X technology cannot meet the ever-growing requirements in the future. Efficient NR access technology, core network capabilities, and edge-cloud services are needed to meet V2X requirements. Kudos goes to the proven history, reliability, and development of cellular technology in telecommunications, cellular technology may resolve the current issues and requirements of V2X communications in vehicular networks.

The 3GPP released Cellular V2X (C-V2X) specification in Rel.14 and Rel.15. The 3GPP introduced the 5G NR technology focusing on further enhancement of the cellular V2X networking infrastructure in Rel.16 [5]. The new 5G NR will be a game changer, because it can supplement or substitute 802.11p in V2X communication. Based on C-V2X, connectivity in vehicular networks can be obtained in the following communication modes:

1. V2I communication mode: in V2I communications, vehicular nodes communicate with the RSUs within communication range. The RSU can be incorporated in either an eNodeB or a stand-alone traffic signal post.
2. V2N communication mode: in V2N mode, vehicular nodes communicate with cellular infrastructures (e.g., eNB), evolved packet switching, remote servers providing extended

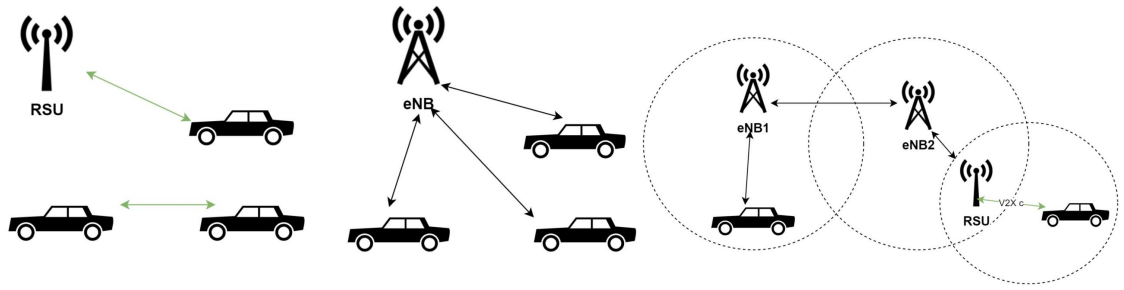
communication between the vehicles, and cloud-based services through cellular networks. V2N allows to broadcast and unicast communications between vehicular nodes and V2X management systems.

3. V2V communication mode: the vehicular nodes communicate with each other at close proximity in an ad-hoc domain, without infrastructures, such as RSUs.
4. V2P communication mode: in V2P mode, vehicles connect with pedestrians or bikers on the road to prevent accidents.

2.1. Types of V2X Communications

The advancements in vehicular communication include various types of communication technology. There are currently two underlying technologies that allow V2X communication, namely IEEE 802.11p and cellular technologies, also known as CV2X. Besides the standard V2X communication, there are few other enabling technologies that are in the process of standardization, such as Visible Light Communications (VLC), mm Wave, etc. The IEEE 802.15.7 VLC Task Group has accomplished MAC and PHY standards for VLC for vehicular networks also known as Vehicular Visible Light Communication (VVLC). Some of its features are VLC spectrum is unlicensed, works in between 380 nm to 780 nm, providing 1000 times higher bandwidth, and being economically feasible. However, VVLC has limitations, such as it only works in visible light and it is heavily impacted by poor weather, rain, fog, obstacles, etc. Hence, it can only be considered as a complementary technology for cellular V2X or IEEE 802.11p, which can be useful in dense and urban location [6,7]. In the recent past, millimeter wave (mmWave) were used for the processing of high-bit rates. The gigabit per second bit rates necessary for the sensor data sharing between the vehicular nodes is not supported in current networks i.e., 802.11p or LTE. The 5G mmWave communications provide higher data transfer rates for a specific vehicle using multiple antenna beamforming. It is also possible to create a new standard or an updated version of the ISO standard [8] with a dedicated spectrum for mmWave V2X communications that is similar to 802.11p, but it may require supplementary equipment to support mmWave V2X communication [9].

In general, V2X communications can be direct communication, fully network-assisted communication, and hybrid communication, as shown in Figure 2. In direct communication, vehicles connect with neighboring vehicles on a peer-to-peer basis. Communication must be carried out via the RSU or Base Station (BS) in fully network-assisted communications. In hybrid communications, vehicles communicate with each other through a combination of direct communication and network-assisted communication by utilizing 802.11p and cellular networks components, such as RSUs and BSs.



(**a**) Direct (802.11p/PC5) (**b**) Full network assisted (**c**) Hybrid (5G+PC5/802.11p)

Figure 2. Different types of Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) scenarios. (**a**) Direct (802.11p/PC5) (**b**) Full network assisted and (**c**) Hybrid (5G+PC5/802.11p).

2.2. State-Of-The-Art V2X Communications

This section presents state-of-the-art and future technologies in V2X communications. We begin with state-of-the-art V2X technologies.

2.2.1. DSRC-Based V2X

The 5.9 GHz DSRC-based V2X provides cooperative awareness applications such as vehicle warning, emergency brake lighting and vehicle platooning. However, such applications are only appropriate for low vehicle-density environments. In fact, hundreds of thousands of vehicles drive on the road and V2X applications need an extremely high capacity, high bandwidth, and very low latency in a densely populated environment. In the case of critical and emergency warning notifications, latency plays a very important role in the security of traffic to prevent collisions. Some of the features and requirements of future V2X are high bandwidth, low delay, high scalability, availability, reliability, and high data speeds. DSRC has limitations to satisfy all of the specifications of future V2X requirements due to weakness in the physical layer (i.e., radio technology) and the absence of collision and interference management. As a result, the realization of V2X in vehicles has been delayed. Moreover, intelligent vehicle connectivity requirements and applications are growing exponentially, while DSRC cannot get closer to the ever-increasing needs of such applications. The infrastructure of DSRC needs RSUs that take a massive amount of time and money for global implementation. DSRC is an asynchronous system that is based on the CSMA/CA protocol, so there are many physical layer inadequacies that result in reduced performance. DSRC based on the CSMA system is more vulnerable to interference, as there is no channel access as long as activity is sensed on the channel. In addition, CSMA issues are more pronounced at higher network loads and are not suitable for critical communication scenarios [10]. On the other side, a different approach based on cellular networks is investigated for V2X connectivity as a candidate technology.

2.2.2. Cellular V2X

The Cellular Vehicle to Everything (C-V2X) was developed by the 3GPP based on V2X RAT in Rel.14 that gives highest priority for modifications of radio access suitable for V2X. LTE for vehicles (LTE-V) was introduced in vehicle networks as an alternative technology for intelligent transport, in addition to DSRC. Telecom companies and the automotive industry approved LTE-V for vehicle connectivity based on LTE. The LTE-V promised low costs, rapid development, and installation by leveraging existing cell towers to make the public transport network more efficient and accessible. Soon, the telecom companies and the automotive industry approved LTE-V for vehicle connectivity based on LTE-A. There is some research on using unlicensed bands in 5G networks via LTE and WLAN aggregation in order to alleviate spectrum scarcity [11,12]. Several vehicles use an on-board system to connect to the cellular network for telematics, GPS systems, infotainment, fleet management, etc.

For commercial applications, such as voice or data access, C-V2X can use V2N mode based on existing licensed cellular networks. The cellular network provides access to the cloud through commercial licensed spectrum using a network slicing architecture for the vertical industry. C-V2X describes transmission modes that allow for direct V2X connections over the PC5 interface through the sidelink channel. The PC5 refers to the point of contact where the vehicular nodes connect with other nodes directly over the same channel, where it does not require connection with the base station. Based on Rel.14 [13] and Rel.15 specification, the 3GPP announced C-V2X technology. The Rel.14 included two additional transmission sidelink modes to enable V2X communications with low latency. The two transmission modes are mode 3 and mode 4, as shown in Figure 3 [14]. The C-V2X can perform in both within-coverage and outside-of-coverage environments, i.e., C-V2X can work with both the conventional LTE air interface and the sidelink air interface [15].

1. V2X based on LTE-Uu Air Interface: LTE-Uu is the standard air interface for connecting User Equipment (UE) and an eNodeB. Each UE that supports the LTE-Uu protocol relays its signal on uplink to the eNB, and the eNB transmits the signal to the destination UE on downlink. The eNB will use semi-persistent scheduling to lower the scheduling overhead that is involved with V2X uplink transmission. In semi-persistent scheduling, the eNB allocates resources to a user

over several subsequent transmissions, as most of the traffic is periodic and has similar packet sizes [16].

2. V2X based on PC5 Air Interface: according to the the 5G Automotive Association (5GAA), the device-to-device communication mode (i.e., PC-5) must be enabled in C-V2X for direct safety message communication assuring privacy. This mode also works well in the ITS 5.9 GHz band without a paid subscription, and provides privacy. In addition, for commercial applications, such as voice or data access, C-V2X can use V2N mode based on existing licensed cellular networks. The PC5 air interface allows for direct UE communications without requiring each packet to proceed through the eNodeB. The user nodes can exploit the PC5 interface when eNodeB is either present or absent.

    - C-V2X sidelink mode 3: in C-V2X side-link mode 3, the scheduled mode functions only in the presence of a base station or an eNB. The allocation of resources is carried out in a centralized manner by the cellular network. Some of the mode 3 mechanisms are semi-persistent scheduling, UE reports based scheduling, and cross carrier scheduling. However, this mode has an issue in high mobility highway scenarios, where the vehicles should be connected with the eNB.
    - C-V2X sidelink mode 4: C-V2X side-link mode 4 functions independently in the absence of eNB support for directly interacting using the PC5 side-link radio interface using a 5.9 GHz frequency band similar to the DSRC. It is also known as autonomous mode. It can interact with other nearby vehicles in a decentralized manner without depending on central cellular network connections. The Mode 4 in C-V2X showed better performance compared to the IEEE 802.11p protocol in several situations during an initial comparison [17]. Moreover, it provides high security for different operating modes.

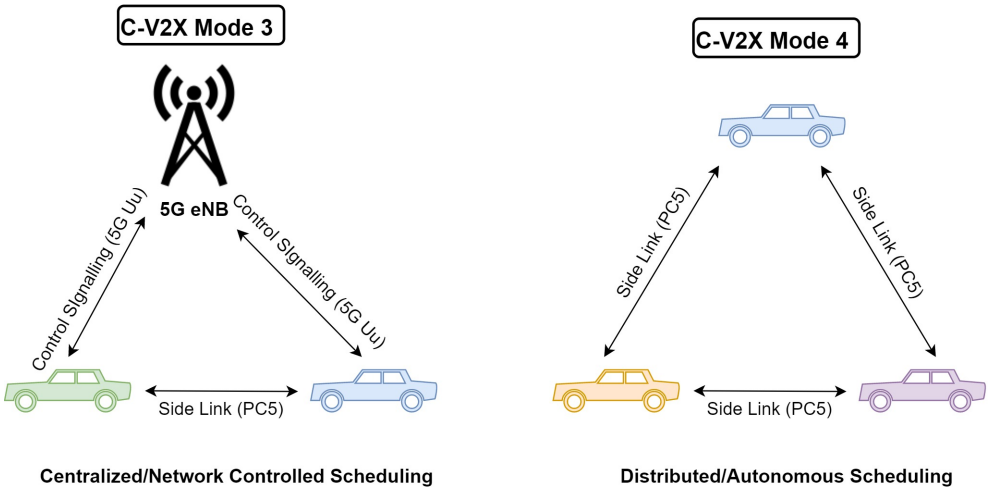


Figure 3. Transmission modes 3 and 4 of Cellular V2X (C-V2X) communications.

2.3. Comparison of State-Of-The-Art V2X Technologies

Table 1 shows a detailed comparison between state-of-the-art C-V2X and DSRC in terms of various components, functions, and mechanisms [18,19]. According to the 5GAA [20], C-V2X can be used for basic safety applications across the world, based on device-to-device connectivity operating on the 5.9 GHz bandwidth, which is a primary typical spectrum. This is one of C-V2X's major advantages over DSRC when it comes to direct communication for interoperable service. Table 1 shows the advantages of C-V2X over IEEE 802.11p (or DSRC) [18].

Table 1. Detailed Comparison of DSRC based and Cellular based V2X communications.

Components	**DSRC V2X**	**Cellular V2X**
Specification Completion	Completed	Rel.14/15 completed & Rel.16 in progress (as of 2019)
Technology	Wi-Fi	LTE/ 4G
Modulation	OFDM	SC-FDM
Retransmission	No HARQ	HARQ
Connectivity	Hybrid mode, i.e., connects with cellular network for non-safety services	Hybrid model, i.e., connects with peer vehicles based on PC5 mode
Network communication	Limited (Via APs only)	Full support
Resource selection	CSMA-CA	Semi persistent Tx with comparative energy-based selection
Line coding	Convolution code	Turbo code
Deployment	Started in 2017. Commercialized in 2019	Mass market distribution in China by the end of 2020
Future guideline	Backward compatible and interoperable upgrade to 802.11bd	C-V2X Rel.16 based on 5G NR and operates on different channel
Latency	Low latency for V2V communications	Round trip latency less than 1ms, minor delay due to centralized communication
Range	Good for short radio range	Good for extended communication
High mobility support	Upto relative speed of 500 km/h with advanced receiver support	Up to 500km/hr as a minimum requirement
High density support	Packet loss at high density	No packet loss guaranteed at high density
Security and Privacy on V2V/ V2I/V2P	Yes (based on IEEE WAVE & ETSI ITS security services)	Yes (based on IEEE WAVE & ETSI ITS security services)
Security and Privacy on V2N	N/A	Yes
Evolution path	Towards 802.11bd	Compatible with Rel -14/15

3. Evolution of V2X Technologies

The state-of-the-art vehicular networking technology, such as IEEE 802.11p and C-V2X, cannot fulfill the demands for next-generation autonomous vehicles that require ultra-reliable communication for critical and safety applications. Thus, the next-generation of intelligent and autonomous vehicles requires enhanced vehicular services that can handle ultra-reliable situations.

The DSRC has been introduced more than a decade ago, which relies on the IEEE 802.11p protocol. The DSRC is suitable for most vehicle-safety applications, vehicle traffic management, and other value-added services, such as parking and vehicle analytics. The global adoption of DSRC has been delayed due to the communication challenges that were introduced by dynamic mobility and poor scalability. Meanwhile, the 3GPP studied the C-V2X based on LTE that provides performance advantages by leveraging the infrastructures within the eNB coverage for effective resource allocation, higher link budget, less interference, and improved Non-Line of Sight (NLoS) capabilities to overcome

the DSRC limitation [21]. The C-V2X sidelink mode 4 performs better than DSRC with regard to higher link budgets as well as frequency re-use over a specified geo-location. However, this mode performs poorly due to the increased interference between user nodes, while reducing the reuse distance when traffic density increases. The DSRC and C-V2X are capable of providing the vehicle safety applications within the message requirements of 1 Hz to 10Hz periodicity and end-to-end latency of 50–100 ms. However, as vehicles become more advanced and, as they evolve towards intelligent and autonomous vehicles, the QoS requirements of V2X become more stringent. Thus, the existing V2X technologies may not satisfy the performance requirement of future V2X communications.

The existing V2X technologies need to evolve in order to enhance the reliability in advanced V2X use-cases for intelligent and autonomous vehicles. They should satisfy ultra-low latency, safety, and security enhancements beyond what the existing V2X applications have achieved based on basic safety applications [22]. The V2X must have a higher reliability for message exchange between the vehicles. The reliability can be maintained by using consistent communication links to reduce risks, such as vehicular crashes. Some of the advanced V2X applications are vehicle platooning, advanced driving, extended sensors, and remote driving. These applications not only improve road safety, but they also improve traffic control and serve the infotainment needs of passengers. Table 2 shows advanced use cases and their QoS requirements based on the reliability of transmitted messages, variable packet sizes, delay requirements, and transmission range.

Table 2. Advanced use cases and Quality of Service (QoS) requirements of Vehicle to Everything (V2X) applications [22].

Use Case	Communication Mode	Pyaload (Bytes)	Max. Delay (msec)	Datarate (Mbps)	Minimum Range (m)	Reliability
Advanced driving	V2V, V2I	300–12,000	3∼100 ms	10–50	360–500	90–99.999
Remote driving	V2N	-	5 ms	UL:25/DL:1	-	99.999
Vehicle platooning	V2V, V2I	50–6000	10∼500 ms	50–65	80–350	90–99.99
Extended sensors	V2V, V2I, V2P	1600	3∼100 ms	10–1000	50–1000	90–99.999

On the other hand, several complex control systems are addressed more commonly, such as safety-critical systems or Cooperative Adaptive-Cruise Control (CACC), which need to be examined independently. Such systems require stringent specifications in the communication network for transmission latency and reliability. Reliable communication is especially challenging for vehicle applications because of the constantly evolving nature of the wireless channel, which results in a constantly outdated channel estimation. Moreover, Inter-Channel Interference (ICI) becomes a bottleneck because of the high Doppler change in V2X scenarios.

3.1. Evolution of Non-Cellular V2X from 802.11p to 802.11bd

The IEEE 802.11p standard was launched in 2010 based on the IEEE 802.11a wireless local area network (WLAN) standard. DSRC performance is adequate for most vehicle safety applications requiring end-to-end latency around 100 ms as long as the vehicle density is low [23]. However, DSRC scalability and performance degrades if the vehicle density increases, which is due to two main factors, i.e., packet collisions from simultaneous transmissions and the hidden node problem.

To overcome these issues, IEEE 802.11 and the 3GPP are focusing on next-generation V2X systems; and, have created a task force called IEEE 802.11 next-generation V2X (NGV). A new and updated IEEE 802.11bd was introduced for V2X communications. IEEE 802.11bd will be an advanced form

of existing 802.11p by leveraging the MAC and PHY options of 802.11n/ac/ax [24,25]. It overcomes the issues related to 802.11p in terms of MAC throughput, interoperability, Doppler shift, etc. Table 3 summarizes the advancements in 802.11bd over 802.11p based on features and mechanisms.

Moreover, the 802.11bd should be able to meet the following requirements:

- Coexistence: the 802.11bd standard must coexist with 802.11p. The 802.11bd should detect the 802.11p data transmissions and comply with channel access and vice-versa.
- Interoperability: the 802.11bd and 802.11p standards must be interoperable i.e., devices, information systems or applications should be interoperable in such a way that 802.11p devices can detect and decode at least one of the transmission modes from 802.11bd devices and vice-versa.
- Fairness: the 802.11bd and 802.11p standards must have fair communication and access capabilities in co-channel configurations.
- Backward compatibility: the 802.11bd must be backward compatible in such a way that at least one mode of 802.11bd must be interoperable with 802.11p.

Table 3. Feature comparison between 802.11bd and 802.11p.

Features/ Mechanisms	**802.11bd**	**802.11p**
Frequency band	5.9 GHz/60 GHz	5.9 GHz
Sub-carrier spacing	312.5 KHz/156.25 KHz/78.125 KHz	156.25 KHz
Channel coding	LDPC	BCC
Re-transmission	Congestion dependent	None
Cyclic Prefix (CP)	1.6 us and 3.2 us	1.6 us
Spatial streams	Multiple	One
Relative vehicle speed	500 km/hr	252 km/h
Doppler shift counter measures	High density midambles	None

Some of the key mechanisms of 802.11bd are as follows:

1. Midambles: the 802.11p PHY layer was extracted directly from 802.11a, decreasing the spacing of the sub-carrier from 312.5 KHz by a factor of two. In 802.11p, the 156.25 KHz subcarrier spacing generated a trade-off between multipath fading and relative Doppler spread for average vehicle speeds [26]. To overcome this issue, the 802.11bd suggests the use of midambles, similar in structure and function to the preamble except for their position within the frame. The preamble, which is at the start of the frame, is used for the initial estimation of channels. In 802.11bd, the midambles can be inserted with appropriate frequency between OFDM data symbols.
2. Re-transmissions: one of the approaches to enhance reliability is to allow one or more packet re-transmissions in both 802.11p and 802.11bd, as shown in Figure 4. For 802.11p applications, the initial transmission and its re-transmissions act as separate packets, and the packets are transmitted successfully as long as one packet is received successfully. Original transmissions and re-transmissions can be either transmitted within the same channel access or by using different contention procedures [27]. In 802.11bd, the Task Group bd (TGbd) introduced an adaptive re-transmission system, where frame re-transmission decisions are based on the level of congestion and the number of re-transmissions [28].

Figure 4. Frame format used for re-transmission in 802.11bd. [27]

3. Alternate OFDM Numerologies: the OFDM performance is based on the ratio of usable symbol length to overall symbol length. The OFDM efficiency increases as subcarrier spacing

decreases since the duration of the cyclic prefix becomes invariant to the duration of the symbol. To improve OFDM performance, the 802.11 TGbd participants are investigating the use of narrow OFDM numerologies (i.e., subcarrier spacing) to maximize the number of subcarriers while also maintaining a 10 MHz channel [29]. Nevertheless, the specification of alternative OFDM numerologies should take into account the maximum relative velocities.

4. Dual Carrier Modulation (DCM): the DCM is a method used in 802.11ax that includes transmitting the same symbol twice over sufficiently distant sub-carriers to achieve frequency diversity [28]. Because each transmission of symbols is repeated over two different sub-carriers, the order of modulation must be doubled to maintain the throughput. The DCM can help boost the efficiency of block-error-rate (BLER) given the rise in modulation order.
5. mmWave Frequencies: the millimeter waves (mmWaves) are usually classified as electromagnetic (radio) waves that lie within the 30–300 GHz frequency spectrum and that can communicate over short distances, but with very high throughput even at lower order MCS (such as video streaming, HD three-dimensional (3D) maps downloading, etc.). The principle for designing mmWave 802.11bd can be legacy 802.11 standards, such as 802.11ad, or its 802.11ay enhancement that already operates within the mmWave bands.
6. Other PHY & MAC mechanisms: other characteristics of the PHY layer being considered for use in 802.11bd include the use of Low Density Parity Check (LDPC) codes and multiple transmit/receive antennas to improve the reliability through multiple antennas or increase throughput by spatial multiplexing [24,29]. The 802.11bd standard will leverage the contention parameters of 802.11p with multiple Enhanced Distributed Channel Access types to ensure equitable and fair channel access options for 802.11bd and 802.11p users at the MAC layer.

3.2. Evolution of Cellular V2X

The incorporation of a mobile network provider for V2N will facilitate the use of frequencies beyond ITS, with high service quality in low bands, and millimeter wave in 5G. It also provides low latency wide area network support for assisted driving. The introduction of NR V2X is not to replace the C-V2X technology that has already been standardized and it serves as a roadmap to commercial deployments. Its aim is to provide support and ensure all V2X applications in C-V2X efficiently. C-V2X and NR V2X are expected to coexist in the same geographic region where new vehicles will have both C-V2X and NR V2X functionality. For this, NR V2X must be able to support not only advanced V2X applications, but also basic safety applications provided by current C-V2X. The NR V2X is designed to support V2X applications that involve different levels and requirements of latency, reliability, and throughput. Table 4 gives the summary of advancements in 5G NR over LTE. Although some of these use cases require periodic traffic transmission, a substantial number of NR V2X use cases are based on efficient aperiodic transmission of messages [15]. Some of the key features and mechanisms of NR V2X are as follows:

1. NR V2X Sidelink Modes: NR V2X defines two side link modes similar to C-V2X. The NR V2X sidelink mode 1 specifies mechanisms, which allows direct vehicle interactions within the coverage of gNodeB. On the other hand, NR V2X side link mode 2 facilitates direct vehicular communications in the out-of-coverage situation.
2. Unicast, Groupcast and Broadcast: in Rel.16, NR V2X supports sidelink unicast, groupcast, and broadcast depending upon the scenarios, such as in-coverage, out of coverage, and partial coverage scenarios. For illustration, a transmitting vehicular node that has a single receiver associated with it can transmit in unicast transmission. A vehicle platoon leader can communicate with other platoon member nodes based on groupcast transmission.
3. NR Numerologies: a main feature included in 3GPP Rel.15 is the provision of adjustable numerologies. In comparison to a single spacing of the sub-carrier used in LTE, NR embraces various spacings in the sub-carrier, which are multiples of the LTE sub-carrier spacing.

The numerology for NR is configured to work with both sub-6 GHz bands and mmWave bands. This is developed by means of multiple numerologies that are formed by the scaling of a fundamental subcarrier spacing (SCS). A scalable OFDM numerology is an improvement introduced in NR, allowing for choice between different subcarrier spacing from 15 KHz up to 480 KHz. The slot length in accordance with these numerologies often varies from 1 ms to 0.031 ms.

4. Slot, Mini-slot, and Multi-slot Scheduling: in LTE, the transmission time is closely coupled to the sub frame duration, i.e., all UEs typically communicate for a duration of 1 subframe (1 msec). Besides this, if the user has only a limited amount of data to transmit, which can be accommodated in less than 14 OFDM symbols. It is inefficient to reserve the entire slot for its transmission. In NR V2X, a mini-slot solution is furnished to transfer data using only two, four, or seven OFDM symbols without any slot limits. In addition, slot aggregation (i.e., adding two or more slots to create a multi-slot) would be provided in NR V2X to account for use-cases that need the sharing of large packets.
5. Channel Coding: as channel coding has a major effect on the reliability, performance and throughput of wireless systems, more effective and consistent coding methods are implemented. The LTE turbo codes are substituted by LDPC coding for data channel and LTE convolution codes are substituted by Cyclical Redundancy Check (CRC) assisted polar codes for the control channel in NR V2X.
6. PHY layer Improvements: NR V2X will provide several other PHY layer improvements, most of which are derived from 5G NR. These involve the use of LDPC coding, higher order MCS like 64-QAM, and a dynamic number of Demodulation Reference Signal (DMRS) symbols per slot.
7. New sub-modes of NR Sidelink Mode 2: unlike C-V2X sidelink mode 4, where there are no sub-modes, the 3GPP started evaluating four new sub-modes of NR V2X sidelink mode 2, i.e., from mode 2 (a) to mode 2(d) [30]. C-V2X sidelink mode 4, resource reservation algorithm leverages the periodicity and fixed-size data of basic safety messages. In general, this presumption is no longer valid for use in NR V2X, so the resource selection process should be re-engineered.

Table 4. Summary of advancement in 5G NR over 4G LTE.

Features	LTE	5G NR
Frequency band	Up to 6 GHz	Up to 5.9 GHz; mmWave (upto 52 GHz)
PHY layer	SC-FDMA	SC-FDMA, OFDM
Carrier aggregation	Up to 32	Up to 16
Digital beamforming	Up to 8 layers	Up to 12 layers
Channel coding	Data: Turbo coding Control: Convolution coding	Data: LDPC coding Control: Polar coding
MCS	QPSK, 16-QAM	QPSK, 16-QAM, 64- QAM
Control & data multiplexing	FDM	TDM
Scheduling interval	One sub-frame	Slot, mini-slot or multi-slot
Side link modes	Modes 3 and 4	Modes 1 and 2
Spectrum occupancy	Up to 90% of channel BW	Up to 98% of channel BW

3.2.1. Evolution from Lte-V2X to 5G NR V2X

In 2016, the 3GPP achieved the first cellular V2X standard called LTE-V2X with Rel.14 [31]. Since then, every subsequent release has been further improved. Similar to the evolution of 3G and 4G; the 5G

NR evolution is part of the ongoing mobile network development process to satisfy the demands of 5G technologies as shown in Figure 5. The central goal of 5G NR evolution is to improve mobile broadband so it is equivalent to a wired infrastructure in terms of low cost, high bandwidth, high performance, and extremely low latency, which can offer faster, highly efficient, and time-critical services.

In 2016, an alliance known as 5G Automotive Association (5GAA) was established by the global industries from automobile, telecom, and IT industries. It is a cross-industry, multinational alliance, which describes the C-V2X platform and its evolution to 5G. The 5GAA goal is to demonstrate the long-term promise of C-V2X capability and provide superior performance and ever-increasing capabilities based on 3GPP cellular technology. Moreover, 5GAA promotes 5G connectivity solutions that help to increase global market penetration, availability, and that facilitate C-V2X standardization.

In March 2017, the 3GPP worked on specialization of C-V2X in Rel.14. Before Rel.15, the 3GPP worked on developing the functionality of LTE in PC5 direct communication and LTE-Uu interfaces. In 2018, 3GPP continued working on the initial standardization process of New Radio for 5G network, as a first step in Rel.15. In June 2018, the 3GPP published the first full 5G NR specification in Rel.15. In 2019, the 3GPP continued to improve C-V2X and expanded standardization research as well as early testing and implementation of 5G NR in Rel.16. Similarly, in Rel.16, 5G NR C-V2X (or 5NX for short), which is based on Rel.14 C-V2X, will support several communication mechanisms such as unicast, broadcast and geocast. The geocast provides a feedback mechanism for higher reliability. If the signal cannot be interpreted by the system, then NACKs are sent over the same radio resources. When compared to the previous Rel.14 i.e., C-V2X, 5NX provides additional features, such as coordinated driving or platooning based on PC5 communications and enhanced situational awareness for safer driving.

In 2019, the standardization of new 5NX radio technology in Rel.16, provided adequate requirements and new possibilities for current and future autonomous driving industries, while, at the same time, retaining backward compatibility. Some recent C-V2X communication capabilities include wide-band transmission for precise vehicle coverage and positioning, revolutionary architectures for ultra-low latency slot structure, scalable OFDM technology, massive MIMO support, etc. The 5NX offers a unifying communication platform for future autonomous vehicles, such as massive IoT, mission critical services, and improved broadband wireless access.

According to the 5GAA, Rel.16 was expected to be finalized in March 2020, with the physical layer specifications previously completed in December of 2019 and the 5NX is expected to be commercialized by 2023. The Rel.17 will be among the primary operations of the 3GPP between 2020 and 2021, with a deadline for conclusion in July 2021 [32].

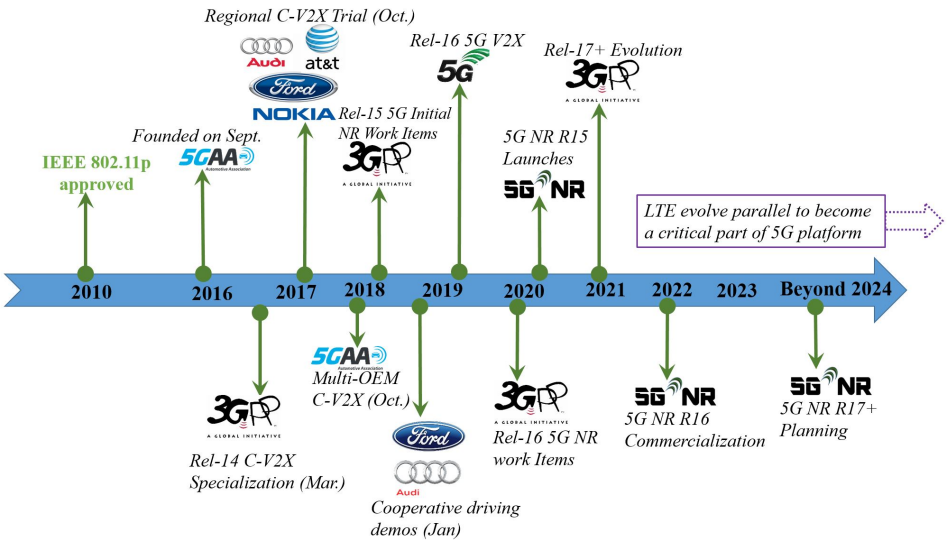


Figure 5. Evolution of C-V2X towards 5G NR V2X [32].

3.2.2. Comparison between Cellular and Non-Cellular V2X Technologies

In a V2V scenario, one of the key challenges to realize ultra-reliable connectivity is the high Doppler shift. The authors in [33] showed that a high Doppler shift causes a high packet error rate, even at a high SNR in case of 802.11bd due to the outdated use of channel estimations combined with deep fades. The results showed that NR V2X can better handle the Doppler shifts, and as a result, it can outperform IEEE 802.11bd based on reliability [33]. The authors tried to enhance 802.11bd efficiency by introducing midambles under high Doppler changes. Moreover, the authors showed that the DCM and range extension mode further improves 802.11bd reliability. While the features in 802.11bd, such as midambles, the extended range preamble, and DCM showed increased reliability; it cannot outperform NR-V2X. The factors behind this are better channel estimations due to high density in the DMRS, lower code rates and SC-FDMA in NR V2X.

The salient features described above make NR V2X more reliable, efficient and flexible compared to other technologies. A comparative summary, including all the common features of 802.11p, 802.11bd, LTE V2X, and NR V2X are given in Table 5 [34,35].

Table 5. An overall comparison of 802.11p, 802.11bd, LTE V2X, and NR V2X based on common features.

Features	802.11p	802.11bd	LTE V2X	NR V2X
Base technology	802.11a/n	IEEE802.11n/ac	4G/LTE	5GNR
Radio bands	5.9 GHz	5.9 GHz, 60 GHz	5.9 GHz	5.9 GHz∼52.6 GHz including mmWave
Channel coding	BCC	LDPC	Data:Turbo coding Control:Convolution coding	Data:LDPC Control: Polar coding
Subcarrier spacing	156.25 KHz	312.5 KHz, 156.25 KHz, 78.15 KHz	15 KHz	Sub-6 GHz:15,30, 60 KHz mmWave:60, 120 KHz
Retransmission	None	Congestion dependent	Blind	HARQ-based
Modes	Broadcast	Broadcast, groupcast	Broadcast	Broadcast, groupcast, unicast
PHY layer	N/A	OFDM	SC-FDMA	SC-FDMA, OFDM
Interoperability	N/A	Yes	N/A	Non co-channel
mmWave support	N/A	Yes	N/A	Yes

4. Edge Computing for V2X Communications

The current cloud computing systems encounter several issues related to security, communication latency and poor performance because of central server architecture. The edge computing helps to solve these issues by installing distributing Multi-access Edge Computing (MEC) servers [36]. The edge computing device is a system that offers a point of access to the core network of the enterprise or service provider. Example devices include routers, network switches, integrated access equipment, etc. MEC is a promising alternative that can shift computing capacities from clouds to edge devices assisting the future vehicular networks. MEC addresses the delay-sensitive network scenarios, providing mobile services at network edges by hosting computer-intensive applications, pre-processing data generated prior to delivery to the cloud, and providing context-aware applications with RAN information [37].

The European Telecommunications Standards Institute (ETSI) published a white paper based on MEC use cases for V2X [36] that analyzed and discussed the features and recommendations of MEC that support V2X applications. It evaluates and identifies the limitation of MEC in supporting V2X applications, and work towards closing the gaps that were found in MEC for V2X applications by

changing existing MEC services or interfaces. ETSI is working on a specification for V2X interoperability in a multi-vendor, multi-network, and multi-access environment. The specifications focus on V2X MEC services that define necessary information for V2X operations, data flows and data formats. Some of the recommendations for V2X MEC features and services are as follows [36]:

- MEC should provide interoperability by allowing exchange of V2X information among vehicles connected through various access technologies or mobile operators or networks.
- MEC should provide service continuity, and access-network coverage across the country and between multi-operators.
- MEC should provide interoperability in a multi-operator environment that enables MEC applications to communicate securely in various systems even in the absence of cellular network.
- MEC should provide secure multi-operator communication between MEC applications with V2X-related core network control functions.
- MEC should provide feedback information from the network to the vehicles in order to guarantee the reliability of the communication channel in supporting V2X functionality.

Globally, sales from connected vehicles are expected to rise five-fold i.e., more than US $ 24 billion by the end of 2025, according to new analysis by Counterpoint's Smart Automotive Service [38]. Each connected vehicle produces about 30 TB of data within a day that requires very high bandwidth. Mobile Cloud Computing (MCC) [39] is the amalgamation of mobile computing and cloud computing in order to overcome the drawbacks of mobile devices. MCC is a powerful computing technology for offloading network traffic and managing network resources. It works in a centralized manner, where the high computation mobile applications are offloaded in the central cloud computing. It is not efficient and not scalable to handle huge amount of vehicular network data. Some of the drawbacks of MCC are as follows. (a) It works in a centralized manner that impose significant costs in terms of energy, bandwidth and time while transmitting data from the vehicles to the clouds or vice versa. (b) It is difficult to manage and update the mobility and location distribution information in real time. (c) MCC servers cannot extract the real time information from the vehicles due to multiple hops from vehicles to RSU to the cloud. As a result, it degrades the user QoS. In 5G-enabled vehicle communications one of the key criteria is low latency. MEC can become a key infrastructure in 5G networks by bringing certain core functionalities close to the edge devices [40]. A detailed comparison between MCC and MEC is given in Table 6.

The authors in [41] integrated the two promising technologies of MEC and Nonorthogonal Multiple Access (NOMA) technologies in 5G V2X to provide extensive connectivity and to support safety-critical and traffic-efficient applications to deal with things, such as road accidents. The integration of MEC and NOMA provides energy-efficient edge computing that copes with the increasing requirements of ubiquitous connectivity. It minimizes the latency between the edge nodes and the MEC. The existing vehicle networks comprise of heterogeneous physical infrastructure and support different network connectivity components with distinct memory and storage capacities, such as access points, end nodes, and edge routers. The MEC enabled vehicular networks consist of a macro cell equipped with computing server to carry out resource-intensive tasks. The RSU and Wi-Fi AP can also be connected to the macro cell. However, the existing cellular system is based primarily on orthogonal multiple access leading to low speed vehicle connection due to the restricted bandwidth [42]. In 5G, NOMA is proposed in order to give large connectivity and minimize access collisions in bandwidth-limited networks like cellular and vehicular networks to allow non-orthogonal channel access through multiplexing either by power domain or code domain. The macrocell transmits signals to several vehicular users and divides the bandwidth into multiple sub-channels in NOMA-based communications between vehicular nodes and macro cell. The vehicular nodes can utilize multiple sub-channels to send the data at a higher data rate. It helps different users to share frequency resources in a non-orthogonal fashion, with the key benefits of increasing bandwidth, connectivity, and energy-efficiency. In 5G, the macrocell behaves as (1) a global router, (2) MEC server, and (3) Software Defined Network (SDN)-based local controller [43].

The authors in [41] aimed to optimize the achievable transfer efficiency by seamlessly combining both cellular and RSU connectivity to offload network traffic by leveraging NOMA and MEC technologies in vehicular communications. The offloading decision is based on a utility function calculation associated with server rewards for message size, offloading costs and message delay. The detailed heuristic system built on NOMA-based offloading system enabled by MEC for vehicular networks can be found in [41].

Table 6. A detail comparison between Mobile Cloud Computing (MCC) and Multi-access Edge Computing (MEC) [41].

Items	MEC	MCC
Architecture	Distributed	Centralized
Operators	Mobile operators	Cloud providers
Target user	Mobile devices	Internet users
Hierarchy	Three-tier	Two-tier
Data storage	Short duration	Long duration
Server nodes	Large in number	small in number
Bandwidth demands	Based on data sent to clouds	Based on data generated by users
Location awareness	Yes	No
Communication overhead	Medium	High
Information access	Localized information	Globalized information
Delay allowance	Lesser than 10ms	Few seconds or greater
Connectivity	Intermittent	uninterrupted
Service provider	Cisco IOx	Amazon, IBM, Microsoft
Environment	Can exist indoors or outdoors	Exists indoor/consumes large space

5. Issues and Challenges in 5G and Edge-Based V2X

It is clear that the introduction of 5G technology and edge computing in vehicular networks support massive data exchanges between vehicles and the edge-clouds based on V2X communications. On one hand, 5G is one of the most important and emerging infrastructures, but it also needs to be the most safe and secure. On the other hand, decentralized MEC effectively provides various advantages, including omnipresent edge computing services, increased scalability, and decreased network complexity operations in order to deal with the proliferation of V2X applications, accelerated demand, and development of 5G services. For 5G-based MEC networks, the primary concern is to prevent system disruption that is caused by an edge node attacks on MEC servers. Hereafter, we discuss the issues and challenges faced by 5G-based MEC in vehicular networks.

5.1. Data Integrity

In vehicular networks, data integrity is a critical issue and inconsiderate verification generates biased data integrity outcomes. In the cloud or at the edge, 5G data storage and analysis creates concerns regarding data integrity. The data outsourced and stored on the edge server gives rise to concerns related to data breaches, data modifications, deletion, or misuse without the user's knowledge. A careful and periodical data verification is required to protect the data integrity from malicious vehicles.

5.2. Data Availability

In 5G-based edge computing, the data may be stored, copied, and/or cached at various sites on the network. As the number of vehicles connected to MEC servers increases, in-network caching, as well as data replication is important for data availability. The large number of connected vehicles hinder real-time data availability of critical information. Moreover, a seamless data availability service is not assured when multiple vehicles request the same information concurrently or if the edge servers are interrupted by cyber-attacks.

5.3. Data Privacy Management

Privacy is of critical importance for the protection of private and sensitive information about the vehicles in 5G V2X based on MEC. The vehicle users sometimes put their trust in MEC data centers trying to manage applications without knowing how information flows and who is actually using their information [44]. If the 5G-based MEC servers are under attack, a huge volume of heterogeneous information may be leaked and vehicle users' privacy may be breached. Some of the privacy problems have been resolved in existing vehicular networks, like the use of a group signature for secure vehicle communications. However, these schemes have to be well exploited before implementing them in 5G-based MEC networks.

5.4. Immutability

In vehicle networks, the distributed storing of 5G data on edge servers, and the processing of information between edge and vehicle users are susceptible to data modification and attacks by adversaries. The attackers can access personal information such as vehicle user information, or location information through unauthorized access and can modify the information. Such attacks can lead to data modifications and mutability of sensitive information. Thus, strong immutability features are required in 5G-based edge computing through technologies such as blockchain.

5.5. Transparency Requirements

In 5G-based edge computing, edge-cloud resource providers have total control of outsourced network information, such as vehicle information, while vehicle users are unaware of it and are unable to monitor the information until it is offloaded to the edge-cloud network. This causes a critical challenge for vehicle users in performing data flow or utilization verification and monitoring, especially in the 5G contexts where transparency between vehicular users are strongly required to guarantee openness and fairness.

5.6. Traceability

The data traceability is one aspect that can be considered for integrated 5G and edge computing. The vehicle mobility and driving path information could become vulnerable to identity leaks. The data tracking for vehicles in vehicular networks should be secure and only a legitimate entity should be able to trace the data, thus maintaining privacy of the users. The existing data traceability is not sufficiently strong and, thus, the shared data resources can be compromised by the malicious entity, or can be used unlawfully. The attackers may act as a legal entity and could eavesdrop and intercept the exchanged messages. They can trace the messages, and then modify, misrepresent, and monitor the traffic behavior [45].

5.7. Heterogeneity and Interoperability

The 5G-based MEC network is highly heterogeneous in design, i.e., operating systems, architectures, radio-based device interfaces, and services. Interoperability issues in edge computing emerge when different edge-cloud service providers interchange data and applications with one another [46]. The issue is not trivial due to the use of different wireless communication modes, different virtualization implementations, or incompatible APIs [47]. There must be a seamless service to retrieve vehicle data from source MEC servers for the target vehicles.

5.8. Low-Latency

The network providers need to offer low-latency network slicing services for enterprise or vehicle users in order to satisfy the MEC application specifications for very low latency, high security, and high reliability. The MEC sliced network consists of 5G base stations (gNBs), a vehicle network (between gNBs and MEC) and User Plane Function (UPF). The network service flows from all of the networking

devices and the vehicular network to reach MEC. The fewer networking devices the packet goes through, the faster the slicing, and the shorter the transmission delay.

5.9. Wireless Resource Management

When incorporating new technologies, such as MEC into 5G V2X, resource allocation strategies tend to be systematic. For instance, to facilitate high-speed transmission of data, two neighbor vehicles may use D2D communication mode to communicate directly with each other. It increases spectral reuse, obtain hop gains and enhance network efficiency. However, D2D connectivity, typically leads to interference in C-V2X induced by the re-use of the bandwidth of the cellular user. Several methods for maximizing the spectrum use have been developed in various settings in order to solve this issue [48]. In the 5G-based MEC, edge computing with fast processing and low latency plays a major role in enhancing the efficiency of vehicle services. The distribution of resources for edge computing is of great significance for increasing QoS and system robustness.

5.10. Resource Scaling

Resource scaling is one of the main functionalities of cloud or MEC computing. It denotes the process of edge/cloud resources being dynamically allocated, such as CPU and memory. This function plays a crucial role, as it leverages the necessary dynamics and elasticity of the network. While considering the 5G Key Performance Indicators (KPIs), such as throughput, latency, reliability massive machine communication, etc., it is important to determine the effects and usefulness of the current resource scaling strategies on V2X network performance.

Most of the above mentioned issues in 5G and edge based MEC in V2X can be solved by integrating Blockchain technology. The blockchain can solve the issues that are related to data integrity, transparency, traceability, and data privacy. The blockchain provides data integrity by using the Merkle Tree. Similarly, DAG and blockchain records the data in immutable manner and ensures that the data are trustable and the records cannot be altered, modified, or deleted. The data availability issue can be solved by storing the data temporarily at the local MEC servers and then utilizing the pre-fetch methods related with the cache. The interoperability issues can be handled using automation tools that are used to handle user side operations related to the cloud service application. The automation tools consists of adapters that works with several cloud services provided by various cloud service providers [49]. The latency can be reduced by integrating 5G networks with high bandwidth MEC, using Virtualized Network Functions (VNF) and implementing efficient offloading algorithms for controlling and managing traffic flow from vehicular nodes to the MEC servers. The distribution of wireless resources in edge computing should be dynamically adjusted without any centrally controlled manager to ensure high QoS. Blockchain is well suited to such instances by offering distributed ledgers to update resources in a fully automated and reliable manner. A research work in used blockchain to build a decentralized resource distribution system that overcomes the weakness of previous systems based on centralized techniques. The scaling issue can be tackled by using vertical and horizontal scaling architecture. In a vertical architecture, several mini resource pools are positioned at the selected edge locations and an efficient task offloading mechanisms is used for locally processing data on the edge device. The scaling issue can be tackled using vertical and horizontal scaling architecture. In vertical architecture, several mini resource pools are positioned at the selected edge locations and an efficient task offloading mechanisms is used for processing data locally on the edge device. Similarly, the horizontal scaling architecture is based on Opportunistic Edge Computing (OEC) [50] that owns the computing resources in a distributed fashion and lease the resources to the system based on short contracts.

6. Blockchain Potential in V2X Networks

Recently, blockchain technology has gained a lot of attention in many fields, because of its ability to build trust in a decentralized manner. The potential of blockchain is huge. Blockchain can work in a decentralized, distributed and autonomous way without the need for third-party service

providers or centralized authorities. A blockchain is simply a publicly distributed database with all the electronic transactions or events registered in a transparent ledger and shared among the participating members [51]. Every other event in the blockchain database is validated by the consensus mechanism in the network [52]. The blockchain offers privacy and anonymity of the user information, as each peer node holds the same copy of the ledger based on secure cryptography. The blockchain is used in various fields outside the domain of cryptocurrencies because of its unique features, such as immutability of data, public verification, transparency, auditability, security, and privacy [53]. Some of the application fields of blockchain are intelligent transport system [54], IoT systems [55], supply chain management, various types of industry [56], food supply chain [57], smart energy [58], healthcare [59], and many more.

6.1. Blockchain Overview

Blockchains are often confused with conventional databases or Distributed Ledger Technology (DLT). There are three main types of blockchains, and they are private, public, and consortium blockchain. In the public blockchain, any node may join or interact in the blockchain network without authorization, and no one has control over the blockchain network [60]. In the private blockchain, permission from the administrator is required in order to join the network and the administrator has control over the activities of the nodes. The private blockchain are not decentralized systems, because there is a strong hierarchy concerning network control. The consortium blockchain is a 'semi-private' network and it has a control user group, which operates through many organizations. In blockchain, consensus is a fault-tolerant technique that is used to achieve the necessary agreement among distributed multiple nodes on a single state of the network. It is a sequence of rules, which define the contributions made by the participating nodes of the blockchain. In [61], different categories of consensus mechanisms that were used in a different types of blockchain were discussed. In addition, smart contract functionality in blockchain provides enhanced security functionality that sets protocols, and provides user data management, decision-making, and access rights monitoring. It is a programmable application that is automatically implemented when a set of predefined conditions is met [62].

6.2. Blockchain as a Security Mechanism in V2X

The existing vehicular networks face several potential security attack surfaces and threats in inter-vehicle and in-vehicle communications, such as cyber-attacks through internet and edge-cloud based connections by using malicious software, passive attacks, tampering the sensor devices, etc. In this paper, we will focus on inter-vehicle communication security. The conventional security and privacy mechanisms are not strong and are inefficient at protecting intelligent and autonomous vehicles because of the differences in their vulnerability to cyber-attacks. In vehicular networks, a large number of vehicles are connected with each other for information exchange, such as accidents, event reports, traffic information, weather information, infotainment messages, etc. It is extremely challenging to realize a centralized vehicular system for managing and processing such a huge amount of data when considering the timely dissemination of information and, at the same time, ensure network scalability [63]. The V2X communications are vulnerable due to the sensitive data sharing between the intelligent vehicles [64,65]. Some of the security requirements of intelligent vehicular systems are as follows:

- Traceability: each participating vehicle should show data provenance to identify the data flow tracing i.e., the source of the information and any changes in ownership during transmission through the transaction.
- Transparency: the information exchanged between participating vehicles, such as critical accident information, traffic-related messages, etc., should be transparent among the member nodes in the blockchain network, except for the private information. This helps legitimate vehicular nodes obtain information regarding traffic situations and lets them respond accordingly.

- Resilience: if a transaction is erroneous or was corrupted, the corruption is immediately evident, and all the vehicles are kept informed of it. A new transaction can be used to resolve an error, as well as the corrupted transactions can be recovered.
- Immutability: this prevents the event or critical messages from being tampered with after they have been registered in the database.

6.2.1. Motivation for Using Blockchain in V2X

Blockchain can fulfill the above requirements by building trust among the peer vehicular nodes in a trustless environment without the presence of a central authority. One of the main features of blockchain is decentralization that maintains and stores the event information in a transparent and immutable manner, and transmits the event information in a timely, secure, and distributed way. The decentralized validation feature is used for rapid validation of exchange messages based on the consensus protocol that helps in timely management of immutable history of accidents or traffic events in vehicular networks. The co-participation of all the vehicles in creating the block based on consensus mechanism makes it more resilient. The inherent features of the blockchain help to obtain the information traceability and transparency in vehicular networks. In case of accident events, the traffic police, law and enforcement department, and the insurance companies can utilize the information stored in the blockchain to resolve the particular events. The participating vehicles can use the event information stored in the blockchain and act accordingly, because the information stored in the blockchain can be considered as the ground truth.

Hence, blockchain provides a series of features, such as protecting the security and privacy of vehicular nodes against different types of advanced cyberattacks. This guarantees resilience and provides immutability of information despite unknown attacks on the vehicular networks. As a number of vehicular nodes join the blockchain networks, they guarantee the resilience of the blockchain system. Even though certain vehicles go offline or become unavailable due to malicious code, malfunctions in vehicles, or cyber threats, the original blockchain would still be available to other member vehicular nodes. All events or transactions in the blockchains are time stamped and authenticated with private keys. The vehicle owners can securely trace the history of transactions and trace events or transactions at any particular time. This tracing capability prevents possible threats or malicious messages in V2X communications, thus securing the network against deceptive attack. An attacker may attempt to de-anonymize the vehicle identity or track the vehicle's private data, which might jeopardize the privacy of the user. The blockchain can secure the anonymity of the user by using the hash function and encrypting sensitive information using asymmetric cryptography. This function also helps each vehicular node to track the provenance or the source of the data. Moreover, the vehicles cannot collude with other neighbor vehicles while generating the hash functions, which prevents the blockchain network from being compromised by a large-scale attack, and provides more security. A lot of research has been done on integrating blockchain into intelligent vehicles for security purposes [66–69]. Because of these capabilities, the use of blockchain as a security mechanism is increasing in V2X networks.

6.2.2. Challenges of Implementing Blockchain in V2X

The use of blockchain in vehicular networks is affected by several challenges and we discuss some of them here. Several new or modified blockchain have been proposed, such as [70,71], to reduce the average puzzle computation time and lower the block message delivery delays in a geographically bounded area, as shown in Table 7. In Ref. [71], a regional blockchain has been proposed to attain 51% attack success probability in terms of several control parameters such as numbers of good vehicle and malicious vehicles, message delivery time, and puzzle computation time that guarantees the stability of blockchain. Similarly, Leiding et.al [70] proposed self-managed and self-organized blockchain-based VANET using concept of an Ethereum blockchain, smart contract, and challenge-based authentication mechanism.

If we try to implement a blockchain using existing vehicular networks, the PoW Puzzle during the mining phase consumes a significant amount of time that is not suitable for time-critical message

dissemination. The blockchain creates a high requirement for computing power and storage capacity for vehicular nodes. The blockchain for vehicular networks still faces challenges, such as timely dissemination of newly mined blocks, message immutability etc., due to the dynamic topology, large geographic areas, and high mobility of vehicles.

Some research has been done in vehicular networks by integrating edge-cloud computing and 5G cellular networks to provide safety, security, privacy and performance improvements in the absence of blockchain technology, as outlined in Table 7. The authors in [72] proposed a new privacy-preserving protocol to improve the security in vehicular networks, by applying the concept of edge-computing based on 5G cellular networks. Their scheme provides an effective privacy preservation technique with an enhanced class security scheme to improve data transmission for road surveillance system. Similarly, the authors in [73] propose 5G-enabled Software Defined Vehicular Networks (5G-SDVNs), where specified SDN functionality is used along with MEC to handle vehicle groups in 5G networks. The authors used an edge-based data dissemination protocol for VANETs in order to improve connectivity, improve resource utilization, reduce communication overhead, and reduce latency. However, the information exchanged between the vehicles is not transparent and traceable. The exchanged information is not resilient and it can be modified by the malicious vehicles. Thus, integrating edge and cellular V2X networks without using blockchain techniques cannot fully satisfy the security requirements of the vehicular networks.

Table 7. A comparative study of blockchain with 5G and edge computing.

Authors	Ref.	Description	Block Chain	MEC	Cellular /5G	System Characteristics
Leiding et al. (2016)	[70]	Proposed a self-managed, Ethereum blockchain-based VANET	Private BC	No	No	Ethereum incorporated with VANET; applications related to traffic regulations, traffic jams, weather etc.
Shrestha et.al (2016)	[71]	Proposed a regional blockchain based VANET to prevent 51% attacks	Regional BC	No	No	Designed regional blockchain to achieve low 51% attack success probability with several control parameters
Rasheed et. al. (2020)	[72]	Presented new privacy-preserving protocol in VANET using 5G-based edge computing	No	MEC	Yes	Effective privacy preservation method, which can be applied by MEC based on 5G-V2X communications architecture with enhanced iCLASC security scheme.
Huang et al. (2017)	[73]	Proposed 5G-enabled SDVNs with MEC to handle vehicle groups in 5G	No	MEC	Yes	VANET integrated with MEC to push the computation from vehicles to the Edge node for improved performance.

6.3. Integrating Blockchain with Mec and 5G Technology in V2X Networks

The integration of the blockchain with MEC and 5G cellular technologies enables next-generation vehicular networks by providing secure vehicular network orchestration, intelligent resource management,

trust management, and enhanced privacy. The edge computing, i.e., MEC reduces the delay and background congestion by computation offloading [74,75] and distributed content caching [76].

6.3.1. Integration of Blockchain with Cellular Technology in V2X

The 5G and beyond technology in next-generationneration vehicular communication is envisaged to provide higher data rate, higher capacity, enhanced QoE, lower operating cost, lower delay, persistent service delivery, massive vehicular node connectivity, and security [77,78]. The evolution of C-V2X towards 5G NR and its implementation in V2X technology was discussed in Section 3. The convergence of blockchain in next-generation vehicular communications based on 5G opens up new opportunities to empower 5G V2X networks, capabilities, applications, and services, as given in Table 8. Some research works are based on the integration of blockchain with cellular networks in V2X communications [79] and [80]. The authors in [79] presented 5G-based vehicular networks that enable technologies, like Content Centric Networking (CCN) based on blockchain for secure vehicular communications. The authors use CCN instead of TCP/IP and allowed blockchains to monitor the confidentiality of information quality, source, and authenticity of information shared among the participating vehicles. It is possible to store the record of the trusted vehicles as well as messages exchanged between the vehicles in the blockchain. The authors mentioned that 5G provides lower latency, edge connection, and higher capacity based on network slicing in the connected vehicles; however; they did not explain much about network slicing, and the lack of a standard consensus protocol for a permissioned blockchain. Similarly, Sandi et al. [80] proposed a primary stage for a blockchain-enabled 5G autonomous vehicular network, and its architecture offering some remarks and discussed the challenges. The authors presented secondary authentication in 5G-based vehicular networks and model inter blockchain communication. However, the authors raised concerns regarding the constraint of short propagation time required by the vehicular networks. They gave remarks that, if each transaction has short propagation delay, then the system can provide fast authentication, but at the cost of selfish mining by PoW consensus because of the huge number of orphaned blocks. On the other hand, if the block generation time is reduced, it degrades the security level, which hampers the blockchain system.

6.3.2. Integration of Blockchain with Mec in V2X

One way to tackle the above issue is to use blockchain integrated with edge computing in vehicular networks without using cellular networks. There are several key enabling technologies, such as mobile edge computing, SDN, Network Function Virtualization (NFV), and D2D communication, which are developed to promote next-generation vehicular communications. The edge computing, such as MEC, Fog, or cloudlets, have emerged as a promising technology to empower vehicular networks and blockchain. In vehicular networks, the blockchain can be used in geo-distributed edge networks to compute heavy computational tasks. The MEC reduces the delay and background congestion by computation offloading [74,75] and distributed content caching [76,81]. By integrating edge-computing and blockchain together with new and emerging vehicular technologies discussed in Section 3, efficient performance, security and privacy can be maintained in the absence of 5G networks and some of them are discussed in Table 8. The authors in [82] proposed a permissioned blockchain between the different elements involved in handling the data obtained from the vehicles for forensics applications. They used decentralized blockchain using Proof of Concept (PoC) consensus mechanism. They used private cloud for data storage to reduce storage space and lower the processing overheads, whereas the authors in [83] applied Vehicular Cloud Computing (VCC) based on permissioned blockchain using Proof of Driving (PoD) consensus to store intelligent vehicle data for privacy. The authors in [84,85] proposed computation offloading and content caching in wireless blockchain networks integrated with MEC. The authors in [85] used Deep Reinforcement Learning (DRL) and permissioned blockchain in vehicular network edge computing. The vehicles and RSU are used as edge servers for intelligent and secure content caching using Proof of Utility (PoU) consensus and DRL mechanism. Similarly,

the authors in [86] proposed a reliable Fog computing framework, where RSUs are employed to offload tasks to neighboring Fog vehicular nodes based on their reputation scores held at a semi-private decentralized blockchain. They used Proof of Elapsed Time (PoET) consensus mechanism for leader selection and a voting mechanism among the consortium members for block validation.

6.3.3. Integration of Blockchain with 5G-Based Edge Computing in V2X

Because of time-varying channels in V2X, dynamic network traffic strict requirements of various new and emerging technologies that cannot attain their full potential individually. Accordingly, all of the above technologies should be integrated and interact with each other to meet the essential demands and critical requirements of the next-generation vehicular networks.

The blockchain enhances the V2X based on 5G and edge computing like MEC. To integrate the MEC and 5G in vehicular networks, several RSUs or 5G RANs can be configured with MEC computing and storage server units. The convergence of these technologies along with the implication of smart city will bring a massive connectivity of vehicles and IoT devices. This will result in a data traffic explosion due to data generate by diverse applications, in order to meet the heterogeneous demands of IoT devices. While using 5G-based edge computing networks, several attack vectors disrupt the MEC services by attacking the edge nodes of the vehicular networks [87]. The main issue with the convergence is to deal with security vulnerabilities from diverse technological fields and provide efficient and lightweight security and privacy schemes. Thus, blockchain promises to deliver a new set of innovative solutions for 5G-based MEC networks and services in order to improve security, privacy, and decentralization. In particular, 5G-based edge network utilizing blockchain can provide services in three major areas, such as networking, processing, and edge computing. There is no doubt that the convergence of these technologies will bring better security features for the next-generation V2X networks.

We focus on four main aspects, including blockchain as security enhancements, task offloading, edge computing, and system performance improvements. A comparative study of blockchain in advanced V2X communications along with 5G-based edge-computing networks is given in Table 8. The authors in [3] studied the security, privacy, and trust issues combined with blockchain in SDN-enabled 5G-VANET. The authors designed trust management system by integrating vehicular networking with the clouds where the real-time video reports, and road condition messages are transmitted to the semi-centralized cloud. The trust management system is combined with the blockchain and utilizes the 5G networks for uploading real-time cloud-assisted video reports to avoid the fake messages. The blockchain is based on combined PoW and PoS consensus mechanism and managed via a peer-to-peer network established by vehicular systems, including OBUs, RSUs, and gNBs. Their simulation results showed that the detection accuracy is decreased as the number of malicious nodes are increased. This can be improved by using MEC based on 5G networks and blockchain in V2X, as proposed by the authors in [88]. We will further elaborate the concept of [88], because this is the only article, to the best of our knowledge, which utilized 5G-based MEC computing and blockchain along with Artificial Intelligence (AI) in V2X networks.

The authors in [88] proposed a novel secure and intelligent architecture for 5G and beyond networks by integrating Deep Reinforcement Learning (DRL) and blockchain into wireless and vehicular networks to enable a flexible and secure resource management, networks orchestration, and enhanced content caching scheme. Their architecture contains three layers viz. user layer, edge layer, and cloud layer. The vehicles use heterogeneous networks that are based on cellular V2X to enhance communication speed, and to provide seamless connection and reliable coverage for autonomous driving. The resource-limited vehicles can offload tasks using the edge or cloud layer that acts as a content caching provider. Blockchain is used on RSUs for providing security and privacy to the critical information shared between vehicles because V2X are operated in trustless environment.

Table 8. A comparative study of Blockchain in advanced vehicular networks with 5G-based edge computing.

Paper	Ref. No.	Description	Blockchain/ Consensus	Edge Comp.	Cellular /5G	System Characteristics
Ortega et al. (2018)	[79]	Presented Content Centric Networking (CCN) based on BC for secure vehicular communications	Permissioned BC	No	Yes	Used CCN instead of TCP/IP & allowed BC to monitor source confidentiality, quality & authenticity of shared data
Rahmadika et al (2019)	[80]	Proposed BC-enabled 5G autonomous vehicular networks	Permissioned BC/ BFT/PoD	No	Yes	Presented secondary authentication in 5G networks & model inter BC comm.
Dorri et al. (2017)	[54]	Proposed a BC-based vehicular networks to protect vehicle privacy & improve security	Public BC managed by overlay nodes	Cloud storage	No	Decentralized security & privacy via overlay networks for smart cars;immune to prevalent security threats
Cebe et al. (2018)	[82]	Proposed a BC for handling vehicle data & forensics applications	Permissioned BC /PoC	Private cloud	No	Used decentralized ledger with reduced storage & consumes low overhead
Liu et al. (2018)	[84]	Proposed computation offloading & content caching in BC with MEC	Public BC /PoW	MEC	No	Used MEC enabled-block chain using two offloading modes;offloadsPoW & content caching using stochastic game theory.
Dai et al. (2020)	[85]	Proposed deep RL & permissioned BC for content caching in edge-based vehicular networks	Permissioned BC/ PoU	MEC	No	Vehicles & RSU acts as edge servers for intelligent content caching; caching at edge are performed by integrating BC using PoU & DLR.
Singh et al. (2017)	[83]	Proposed an intelligent vehicles data sharing framework based on BC	Permissioned BC /PoD	VCC	No	Seven-layer conceptual structure layout compatible with real-time traffic information
Iqbal et al. (2020)	[86]	Proposed Fog-computing using RSUs to offload tasks to neighboring fog vehicles, based on reput ation scores held at BC	semi-private consortium/ PoET	Fog	No	System maintains BC at RSUs, retaining a social reputation in VANET. Evaluate system based on task completion, end-to-end delay & queuing delay.
Xie et al. (2019)	[3]	Investigates security,privacy & trust issues combined with BC in SDN-enabled 5G-VANET.	PoW + PoS	Cloud -based	Yes	BC is maintained by OBUs,RSUs and gNBs that records all road information & maintains trust management to evade fake msg.
Dai et al. (2019)	[88]	Proposed a secure and intelligent architecture for 5G & beyond networks by integrating deep RL & BC in V2X.	Consortium BC /PoW	MEC	Yes	Adopt BC-enabled resource management, spectrum sharing, content caching, & offload computation. Max. system utility by sharing problem in BC empowered by DRL in 5G VANET.

The edge layer consists of 5G network infrastructures, like the Macro BS (MBS), small BS (SBS), and RSUs, which are geo-distributed and installed with MEC servers and blockchain platforms. MEC reduces latency and prevents back haul congestion by offloading computation and caching content in distributed manner. Each BS or RSU supports blockchain to allow untrustworthy vehicles to communicate securely for content caching or storing critical messages as transactions. The cloud layer has a global view of the network that consists of high computing servers, but long distance between vehicle and cloud causes delay. The advantage of this hierarchical scheme is that it intelligently and securely manages the resources in an optimal way by leveraging the new paradigm such as AI and blockchain technology. The AI based on DRL effectively evaluates the topology, channel distribution, and existing wireless network congestion effectively. MEC incorporated with blockchain and AI facilitate reliable network diagnosis and enable dynamic orchestration. This scheme helps to reduce the block generation time as well as block propagation delay as the transaction messages are exchanged near the edge nodes.

7. Open Issues and Future Research Directions

This section provides a variety of critical open issues and research concerns that should be addressed carefully during the system design as discussed below.

7.1. Performance and Scalability Issues

Besides the advantages of blockchain scalability and performance issues are still major obstacles in the integrated ecosystems. The scalability issues are mainly based on storage, throughput, and networking.

- Storage: a massive volume of data transactions such as information storage, management of resources and vehicle transactions are generated due to the integration of blockchain in 5G-based MEC in vehicular networks. In conventional blockchain, all of the nodes store a copy of complete blockchain transactions. As a result, the blockchain bloats and results in a computational and storage load on resource-constrained vehicles [89].
- Throughput: the performance concerns include limited throughput in terms of number of transactions per second, and delays that are scaused by additional time to add block transactions into the blockchain [90]. The blockchain has limited block size, and the block generation time grows rapidly due to long waiting time for transactions to be added on the chain that results in limited throughput.
- Network Resource: in the context of integrated blockchain and 5G-based MEC environments, high density networks with large number of heterogeneous and resource constrained devices, consume lots of resources. It might be difficult to fulfill the resource requirements of blockchain in order to accomplish large-scale transaction processing. Moreover, the blockchain consumes large network resources in terms of transmission power, mining, and bandwidth based on the consensus mechanism that results in high latency [91].
- Blockchain Incentive and Penalty Mechanisms: an efficient incentive mechanism should be built so that the incentives are assigned to the miners in a fair manner. Thus, a future direction for research is to develop an efficient and robust incentive mechanism with fair distribution to encourage all parties and miners to engage in the blockchain. In addition, penalty systems are also necessary to discourage any malicious entity from performing harmful activities.

Besides the above-mentioned issues, a lot of research needs to be done to improve blockchain performance and scalability from various design viewpoints, such as hardware mining [92], hybrid consensus mechanisms [93], off-chain [94], and on-chain [95], solutions, standardization, and regional blockchain design [71].

7.2. Security and Privacy Issues

The vehicle platooning and collaborative control are important aspects of future autonomous vehicles. However, there are security issues and vulnerabilities that exist in application, and networks layers in autonomous platooning, such as message spoofing, DoS, burst transmission, etc. These cyber security issues can be resolved by integrating synchronisation-based control techniques that implements a decentralized detection method to cope with several malicious activities [96,97].

Even though blockchain is considered as a secured distributed ledger, there are certain privacy and security issues in an integrated blockchain. One of the weaknesses is 51% attack vulnerabilities where the attackers modify transaction orders, disrupt mining operations, or trigger double-spending attacks that hamper the blockchain network [98]. Moreover, an attack on a smart contract might result in the leakage of private information about the vehicles, or system logic alterations. Some of the examples of security flaws in integrated blockchain in 5G-based MEC are time-stamping dependency, mismanaged exceptions, and re-entry attacks on smart contracts. Another issue is that anonymous nodes can act as a legitimate network member and perform edge data processing, but they might access

personal information of the vehicles that leads to a privacy issue. While blockchain uses encryption and digital signature to maintain transactions, recent analytical results [99] reveal that transactions can be disclosed during blockchain formation showing that blockchain data security is not very robust in practice. In addition, hackers can exploit smart contracts for illicit activities, causing sensitive data leaks, e.g., cryptographic keys.

Some research results help to address security issues to enhance the overall performance of the integrated ecosystem, such as SmartPool [100], which implements a mining pool to improve transaction verification that overcomes 51% attack vulnerability. More recently, researchers presented an effective security assessment for examining and preventing potential threats, which ensures trustworthy smart contract execution under blockchain [101,102].

7.3. Quality of Service (QoS) Issue

The integration of blockchain in 5G-based MEC environments can introduce novel QoS issues, which would adversely affect the overall system performance of V2X networks. The data traffic generated from the integrated technologies needs to be managed efficiently to reduce latency, and to handle network resources in order to achieve good QoS. One of the most critical goals of future C-V2X based blockchain is to provide high QoS and ultra-low latency for vehicles to satisfy the demands from increased traffic and new services. A solution based on 5G network virtualization was studied in [103] in order to solve blockchain scalability and improve system performance by separating blockchain management from transaction processing in order to reduce the latency and enhance the QoS of blockchain operations. Blockchain requires extensive resources in storage, processing, and network bandwidth to accomplish the consensus process. Without proper planning, the integrated blockchain in 5G-based MEC environments will lead to the deterioration of QoS due to high latency, high energy usage, high demands for bandwidth, and dense network congestion.

Some techniques were presented to solve the QoS issues from two perspectives: (1) lightweight blockchain designs, as discussed in [104–108] reducing the consensus mechanism computation in blockchain and (2) computation offloading as mentioned in [109–111] that is based on integrated 5G technologies with edge computing along with SDN, NFV and D2D communications.

7.4. Future Research Directions

7.4.1. Integrated Blockchain, 5G-Based Mec and Big Data

In the big data era, a large volume of multimedia data generated from integrated 5G-based MEC and V2X nodes could be used for data-related applications such as data mining, machine learning-based data extraction [112]. Nonetheless, big data analytics on 5G-based MECs will pose a range of threats, ranging from data privacy leakage, cyber-attacks, and access control to security breaches leading to extremely advanced data theft [113]. The blockchain can solve major related security vulnerabilities by eliminating the fear of security bottlenecks. The blockchain can facilitate decentralized data sharing that allows large-scale big data deployments in 5G V2X [114]. Many of the research results suggest that blockchain can offer multiple benefits in terms of security, privacy preservation and performance enhancement in big data analytics in 5G-based system [115,116].

7.4.2. Blockchain beyond 5G

Beyond 5G, or specifically 6G, is anticipated to give superior performance to fulfill the extremely high demands from fully autonomous vehicles, by mobile, wearable, IoT networks, and by deep under water communications, etc. It can provide super high throughput, ultra-high reliability, low energy consumption, massive connection, ultra-low latency, space communications, etc. [117,118]. However, like other technologies, 6G will have to cope with a number of stringent technical demands, particularly for tight security and full privacy. Blockchain will play a key role in promoting and enhancing security, and in transforming the future of 6G networks [119].

7.4.3. Machine Learning Integrated with Blockchain for 5G-Based Mec

Machine Learning (ML) techniques create new opportunities for the existing and future V2X technologies, enabling them to learn from data, provide predictions and support decisions [120]. In the integrated system, the ML transforms the way data analytics are performed to help intelligent services, such as traffic data estimation, for avoiding network congestion. There is a lot of research based on integrating machine learning such as DRL with blockchain, 5G-based edge computing in V2X to ensure security, and intelligent resource management [88] in dynamic vehicular network with high mobility. The DRL helps in analyzing the channel interference, channel assignments, and wireless network topology. It helps to choose the most suitable access mode, such as cellular or V2V, to enhance the V2X connection or improve the intelligent vehicle experience. However, the resolution on offloading optimization needs to be further researched to balance the integrated blockchain and 5G-based edge computing.

8. Conclusions

In this survey, we discussed the possibilities provided by advanced V2X networks for safe and secure future autonomous driving. We presented state-of-the-art V2X through a comprehensive literature survey in the related research area. We particularly highlighted evolution towards future V2X based on the 802.11bd and 5G NR. We discussed the issues and challenges in existing V2X based on 5G and edge computing. Apparently, blockchain has emerged as a promising technology to solve the majority of issues and challenges related to privacy, security and networking faced by the existing and next-generation V2X technologies. We examined and explored, in detail, the convergence of blockchain in next-generation V2X communications that opens up new opportunities to empower advanced V2X networks, capabilities, applications, and services. We then investigated the integration of blockchain in 5G-based MEC vehicular networks for security, privacy protection, and content caching. Lastly, we mentioned numerous open research challenges and prospective paths for future research direction on the integrated emerging technologies, such as big data, machine learning, and beyond 5G.

Funding: This research was supported in part by Basic Science Research Program through National Research Foundation of Korea (NRF) funded by the Ministry of Science and ICT (2020R1A2C1010366, 2015R1D1A1A01058595). This research was supported in part by the MSIT(Ministry of Science and ICT), Korea, under the ITRC(Information Technology Research Center) support program(IITP-2020-2016-0-00313) supervised by the IITP(Institute for Information & communications Technology Planning & Evaluation).

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

References

1. US Department of Transportation (DoT). Connected Vehicles. 2020. Available online: https://www.its.dot.gov/cv_basics/cv_basics_what.htm (accessed on 17 February 2020).
2. Sjoberg, K.; Andres, P.; Buburuzan, T.; Brakemeier, A. Cooperative Intelligent Transport Systems in Europe: Current Deployment Status and Outlook. *IEEE Veh. Technol. Mag.* **2017**, *12*, 89–97. [CrossRef]
3. Xie, L.; Ding, Y.; Yang, H.; Wang, X. Blockchain-Based Secure and Trustworthy Internet of Things in SDN-Enabled 5G-VANETs. *IEEE Access* **2019**, *7*, 56656–56666. [CrossRef]
4. ETSI. Technical Specification Group Services and System Aspects. In *Security Aspect for LTE Support of Vehicle-to-Everything (V2X) Services*; Technical Report; 3GPP TS 33.185 V14.1.0.; ETSI: Sophia Antipolis Cedex, France, 2017.
5. 3GPP. Technical specification group services and system aspects. In *Study on Architecture Enhancements for EPS and 5G System to Support Advanced V2X Services*; Technical Report; 3GPP TR 23.786 v0.8.0.; 3GPP: Sophia Antipolis Valbonne, France, 2018.
6. Bazzi, A.; Masini, B.M.; Zanella, A.; Calisti, A. Visible light communications as a complementary technology for the internet of vehicles. *Comput. Commun.* **2016**, *93*, 39–51. [CrossRef]
7. Masini, B.M.; Bazzi, A.; Zanella, A. Vehicular Visible Light Networks for Urban Mobile Crowd Sensing. *Sensors* **2018**, *18*, 1177. [CrossRef]

8. ISO. Technical Committee ISO/TC 204. *Intelligent Transport Systems—Communication Access for Land Mobiles (CALM)—Millimetre Wave Air Interface*; ISO: Geneva, Switzerland, 2012.
9. Choi, J.; Va, V.; Gonzalez-Prelcic, N.; Daniels, R.; Bhat, C.R.; Heath, R.W. Millimeter-Wave Vehicular Communication to Support Massive Automotive Sensing. *IEEE Commun. Mag.* **2016**, *54*, 160–167. [CrossRef]
10. Khairnar, V.D.; Kotecha, K. Performance of Vehicle-to-Vehicle Communication using IEEE 802.11p in Vehicular Ad-hoc Network Environment. *Int. J. Netw. Secur. Its Appl.* **2013** , *5*, 143–170. [CrossRef]
11. Bajracharya, R.; Shrestha, R.; Jung, H. Future Is Unlicensed: Private 5G Unlicensed Network for Connecting Industries of Future. *Sensors* **2020**, *20*, 2774. [CrossRef]
12. Bajracharya, R.; Shrestha, R.; Ali, R.; Musaddiq, A.; Kim, S.W. LWA in 5G: State-of-the-Art Architecture, Opportunities, and Research Challenges. *IEEE Commun. Mag.* **2018**, *56*, 134–141. [CrossRef]
13. ETSI. Digital cellular telecommunications system (Phase 2+) (GSM) TR21.914. In *Release Description; Release 14*; Technical Report; ETSI: Sophia Antipolis Cedex, France, 2017.
14. 3GPP. *Technical specification Group Radio Access Network. Evolved Universal Terrestrial Radio Access (E-UTRA); Physical layer procedures, Rel.15, TR 36.213 v15.3.0*; Technical Report; 3GPP: Sophia Antipolis Valbonne, France, 2018.
15. Naik, G.; Choudhury, B.; Park, J.M. IEEE 802.11bd 5G NR V2X: Evolution of Radio Access Technologies for V2X Communications. *IEEE Access* **2019**, *7*, 70169–70184. [CrossRef]
16. 3GPP. 3GPP TR 36.885—Study on LTE-Based V2X Services. 2016. Available online: https://itectec.com/archive/3gpp-specification-tr-36-885 (accessed on 25 May 2020).
17. Haider, A.; Hwang, S.H. Adaptive Transmit Power Control Algorithm for Sensing-Based Semi-Persistent Scheduling in C-V2X Mode 4 Communication. *Electronics* **2019**, *8*, 846. [CrossRef]
18. 5G Automotive Association. The Case for Cellular V2X for Safety and Cooperative Driving. In *5GAA Whitepaper*; 5G Automotive Association: Munich, Germany, 2016; pp. 1–8.
19. Autotalks. DSRC vs. C-V2X for Safety Applications. 2019. Available online: https://www.auto-talks.com/technology/dsrc-vs-c-v2x-2. (accessed on 1 Novermber 2019).
20. 5GAA. 5GAA: Paving the Way towards 5G. Available online: https://5gaa.org/5g-technology/paving-the-way (accessed on 17 February 2020).
21. Conway, S. V2X Technology Benchmark Testing. Available online: https://ecfsapi.fcc.gov/file/10927105022769/5GAA%209.25.18%20Ex%20Parte%20Notice.pdf (accessed on 20 May 2020).
22. 3GPP. *Study on Enhancement of 3GPP Support for 5G V2X Services*; Technical Report 22.886, G.T.; 3GPP: Sophia Antipolis Valbonne, France, 2016
23. Hassan, M.I.; Vu, H.L.; Sakurai, T. Performance Analysis of the IEEE 802.11 MAC Protocol for DSRC Safety Applications. *IEEE Trans. Veh. Technol.* **2011**, *60*, 3882–3896. [CrossRef]
24. Cao, R.; Zhang, H.; Sharma, P. Potential PHY Designs for NGV. IEEE 802.11-19/0016r0, 01. 2020. Available online: https://mentor.ieee.org/802.11/documents?n=2&is_dcn=ngv (accessed on 17 March 2020).
25. Sun, B. 802.11 NGV Proposed PAR. 2020. Available online: https://www.ieee802.org/11/Reports/tgbd_update.htm (accessed on 19 March 2020).
26. Cheng, L.; Henty, B.E.; Cooper, R.; Stancil, D.D.; Bai, F. A Measurement Study of Time-Scaled 802.11a Waveforms Over The Mobile-to-Mobile Vehicular Channel at 5.9 GHz. *IEEE Commun. Mag.* **2008**, *46*, 84–91. [CrossRef]
27. Fischer, M.; Filippi, A.; Martinez, V. *Additional Details About Interoperable NGV PHY Improvements*; NXP: Austin, TX, USA, 2018; pp. 1–16.
28. Fischer, M. *IEEE 802.11-18/1186r0: Interoperable NGV PHY Improvements*; Technical Report; NXP: Austin, TX, USA, 2018.
29. Cao, R; Zhang, H.; Sharma, P. *Doppler Impact on OFDM Numerology for NGV*; Marvell: Santa Clara, CA, USA, 2018. Available online: https://mentor.ieee.org/802.11/documents?is_group=0ngv (accessed on 10 September 2018).
30. Intel Corporation. *R11809867: Offline Summary for NR-V2X Agenda Item—7.2.4.1.4 Resource Allocation Mechanism*; Technical Report; Intel Corporation: Gothenburg, Sweden, 2018.
31. 3GPP. *3GPP: Initial Cellular V2X Standard Completed*; 3GPP: Sophia Antipolis Valbonne, France, 2017. Available online: https://www.3gpp.org/newsevents/3gppnews/1798v2x (accessed on 19 July 2020).
32. 5G Americas. *5G-Evolution-3GPP-R16-R17*; Technical Report; 5G Americas: Bellevue, DC, USA, 2020.

33. Anwar, W.; Traßl, A.; Franchi, N.; Fettweis, G. On the Reliability of NR-V2X and IEEE 802.11bd. In Proceedings of the 2019 IEEE 30th Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC), Istanbul, Turkey, 8–11 September 2019; pp. 1–7. [CrossRef]
34. Mukherjee, A. *5G New Radio: Beyond Mobile Broadband*; Artech House: London, UK, 2019.
35. IEEE. 3GPP Release 15 Overview. 2020. Available online: https://spectrum.ieee.org/telecom/wireless/3gpp-release-15-overview (accessed on 15 May 2020).
36. ETSI. *Multi-access Edge Computing (MEC): Study on MEC Support for V2X Use Cases*; Technical Report; ETSI: Sophia Antipolis Cedex, France, 2018.
37. Maharjan, S.; Zhu, Q.; Zhang, Y.; Gjessing, S.; Basar, T. Dependable Demand Response Management in the Smart Grid: A Stackelberg Game Approach. *IEEE Trans. Smart Grid* **2013**, *4*, 120–132. [CrossRef]
38. Madhok, A. *Global Connected Car Revenues to Grow Five-Fold by 2025*; Counterpoint: Hong Kong, China, 2019. Available online: https://www.counterpointresearch.com/connected-car-revenues-grow-five-fold-2025
39. Al-Omary, A. A Secure Framework for Mobile Cloud Computing. In Proceedings of the 2019 International Conference on Innovation and Intelligence for Informatics, Computing, and Technologies (3ICT), Sakhier, Bahrain, 22–23 September 2019; pp. 1–6. [CrossRef]
40. Shah, S.A.A.; Ahmed, E.; Imran, M.; Zeadally, S. 5G for Vehicular Communications. *IEEE Commun. Mag.* **2018**, *56*, 111–117. [CrossRef]
41. Ning, Z.; Wang, X.; Huang, J. Mobile Edge Computing-Enabled 5G Vehicular Networks: Toward the Integration of Communication and Computing. *IEEE Veh. Technol. Mag.* **2019**, *14*, 54–61. [CrossRef]
42. Zhang, Y.; Yu, R.; Xie, S.; Yao, W.; Xiao, Y.; Guizani, M. Home M2M networks: Architectures, standards, and QoS improvement. *IEEE Commun. Mag.* **2011**, *49*, 44–52. [CrossRef]
43. Zhang, Y.; Yu, R.; Nekovee, M.; Liu, Y.; Xie, S.; Gjessing, S. Cognitive machine-to-machine communications: Visions and potentials for the smart grid. *IEEE Netw.* **2012**, *26*, 6–13. [CrossRef]
44. Li, J.; Wu, J.; Chen, L. Block-secure: Blockchain based scheme for secure P2P cloud storage. *Inf. Sci.* **2018**, *465*, 219–231. [CrossRef]
45. Liu, H.; Zhang, P.; Pu, G.; Yang, T.; Maharjan, S.; Zhang, Y. Blockchain Empowered Cooperative Authentication With Data Traceability in Vehicular Edge Computing. *IEEE Trans. Veh. Technol.* **2020**, *69*, 4221–4232. [CrossRef]
46. Musaddiq, A.; Ali, R.; Bajracharya, R.; Qadri, Y.A.; Al-Turjman, F.; Kim, S.W. *Trends, Issues, and Challenges in the Domain of IoT-Based Vehicular Cloud Network BT—Unmanned Aerial Vehicles in Smart Cities*; Springer: Cham, Switzerland, 2020; pp. 49–64. [CrossRef]
47. Lewis, G.A. Role of Standards in Cloud-Computing Interoperability. In Proceedings of the 2013 46th Hawaii International Conference on System Sciences, Maui, HI, USA, 7–10 January 2013; pp. 1652–1661.
48. Asadi, A.; Wang, Q.; Mancuso, V. A Survey on Device-to-Device Communication in Cellular Networks. *IEEE Commun. Surv. Tutor.* **2014**, *16*, 1801–1819. [CrossRef]
49. Cloud Standards Customer Council. *Interoperability and Portability for Cloud Computing: A Guide Version 2.0*; Technical Report; Object Management Group (OMG): Milford, CT, USA, 2017.
50. Olaniyan, R.; Fadahunsi, O.; Maheswaran, M.; Zhani, M.F. Opportunistic Edge Computing: Concepts, opportunities and research challenges. *Future Gener. Comput. Syst.* **2018**, *89*, 633–645. [CrossRef]
51. Shrestha, R.; Kim, S. Integration of IoT with blockchain and homomorphic encryption: Challenging issues and opportunities. In *Advances in Computers*; Kim, S., Deka, G.C., Zhang, P., Eds.; Elsevier: Amsterdam, The Netherlands, 2019; Volume 115, pp. 293–331. [CrossRef]
52. Shrestha, R.; Bajracharya, R.; Nam, S.Y. Blockchain-based Message Dissemination in VANET. In Proceedings of the 2018 IEEE 3rd International Conference on Computing, Communication and Security (ICCCS), Kathmandu, Nepal, 25–27 October 2018; pp. 161–166.
53. Singh, M.; Kim, S. Branch based blockchain technology in intelligent vehicle. *Comput. Netw.* **2018**, *145*, 219–231. [CrossRef]
54. Dorri, A.; Steger, M.; Kanhere, S.; Jurdak, R. BlockChain: A distributed solution to automotive security and privacy. *IEEE Commun. Mag. Mag.* **2017**, *55*, 119–125. [CrossRef]
55. Makhdoom, I.; Abolhasan, M.; Abbas, H.; Ni, W. Blockchain's adoption in IoT: The challenges, and a way forward. *J. Netw. Comput. Appl.* **2019**, *125*, 251–279. [CrossRef]
56. Li, Z.; Kang, J.; Yu, R.; Ye, D.; Deng, Q.; Zhang, Y. Consortium Blockchain for Secure Energy Trading in Industrial Internet of Things. *IEEE Trans. Ind. Inform.* **2018**, *14*, 3690–3700. [CrossRef]

57. Tian, F. An agri-food supply chain traceability system for China based on RFID & blockchain technology. In Proceedings of the 2016 13th International Conference on Service Systems and Service Management (ICSSSM), Kunming, China, 24–26 June 2016; pp. 1–6. [CrossRef]
58. Gao, J.; Asamoah, K.O.; Sifah, E.B.; Smahi, A.; Xia, Q.; Xia, H.; Zhang, X.; Dong, G. GridMonitoring: Secured Sovereign Blockchain Based Monitoring on Smart Grid. *IEEE Access* **2018**, *6*, 9917–9925. [CrossRef]
59. Mubarakali, A.; Bose, S.C.; Srinivasan, K.; Elsir, A.; Elsier, O. Design a secure and efficient health record transaction utilizing block chain (SEHRTB) algorithm for health record transaction in block chain. *J. Ambient. Intell. Humaniz. Comput.* **2019**. [CrossRef]
60. Chen, B.; He, D.; Kumar, N.; Wang, H.; Choo, K.R. A Blockchain-Based Proxy Re-Encryption with Equality Test for Vehicular Communication Systems. *IEEE Trans. Netw. Sci. Eng.* **2020**. [CrossRef]
61. Shrestha, R.; Bajracharya, R.; Shrestha, A.; Nam, S.Y. A New-Type of Blockchain for Secure Message Exchange in VANET. *Digit. Commun. Netw.* **2020**, *6*, 177–186. [CrossRef]
62. Buterin, V. A Next-generation Smart Contract and Decentralized Application Platform. In *When Satoshi Nakamoto*; Ethereum Foundation; 2015, pp. 1–36. Available online: https://blockchainlab.com/pdf/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf (accessed on 19 July 2020).
63. Shrestha, R.; Bajracharya, R.; Nam, S.Y Centralized Approach for Trustworthy Message Dissemination in VANET. In Proceedings of the NOMS 2018—2018 IEEE/IFIP Network Operations and Management Symposium, Taipei, Taiwan, 23–27 April 2018.
64. Park, J.H.; Park, J.H. Blockchain Security in Cloud Computing: Use Cases, Challenges, and Solutions. *Symmetry* **2017**, *9*, 164. [CrossRef]
65. Kim, S. *Blockchain for a Trust Network Among Intelligent Vehicles*, 1st ed.; Elsevier Inc.: Amsterdam, The Netherlands, 2018; Volume 111. [CrossRef]
66. Singh, M.; Kim, S. Trust Bit: Reward-based intelligent vehicle commination using blockchain paper. In Proceedings of the 2018 IEEE 4th World Forum on Internet of Things (WF-IoT), Singapore, 5–8 February 2018; pp. 62–67. [CrossRef]
67. Kim, M.; Jang, I.; Choo, S.; Koo, J.; Pack, S. Collaborative security attack detection in software-defined vehicular networks. In Proceedings of the 2017 19th Asia-Pacific Network Operations and Management Symposium (APNOMS), Seoul, Korea, 27–29 September 2017; pp. 19–24. [CrossRef]
68. Kim, S.; Deka, G.C. *Advanced Applications of Blockchain Technology*; Springer: Singapore, 2020. [CrossRef]
69. De La Torre, G.; Rad, P.; Choo, K.K.R. Driverless vehicle security: Challenges and future research opportunities. *Future Gener. Comput. Syst.* **2018**, *108*, 1092–1111. [CrossRef]
70. Leiding, B.; Memarmoshrefi, P.; Hogrefe, D. Self-managed and blockchain-based vehicular ad-hoc networks. In Proceedings of the 2016 ACM International Joint Conference on Pervasive and Ubiquitous Computing Adjunct—UbiComp '16, Heidelberg, Germany, 12–16 September 2016; pp. 137–140. [CrossRef]
71. Shrestha, R.; Nam, S.Y. Regional Blockchain for Vehicular Networks to Prevent 51% Attacks. *IEEE Access* **2019**, *7*, 95033–95045. [CrossRef]
72. Rasheed, I.; Zhang, L.; Hu, F. A privacy preserving scheme for vehicle-to-everything communications using 5G mobile edge computing. *Comput. Netw.* **2020**, *176*, 1–12. [CrossRef]
73. Huang, X.; Yu, R.; Kang, J.; He, Y.; Zhang, Y. Exploring Mobile Edge Computing for 5G-Enabled Software Defined Vehicular Networks. *IEEE Wirel. Commun.* **2017**, *24*, 55–63. [CrossRef]
74. Dai, Y.; Xu, D.; Maharjan, S.; Zhang, Y. Joint Computation Offloading and User Association in Multi-Task Mobile Edge Computing. *IEEE Trans. Veh. Technol.* **2018**, *67*, 12313–12325. [CrossRef]
75. Dai, Y.; Xu, D.; Maharjan, S.; Zhang, Y. Joint Load Balancing and Offloading in Vehicular Edge Computing and Networks. *IEEE Internet Things J.* **2019**, *6*, 4377–4387. [CrossRef]
76. Chen, M.; Hao, Y.; Hu, L.; Hossain, M.S.; Ghoneim, A. Edge-CoCaCo: Toward Joint Optimization of Computation, Caching, and Communication on Edge Cloud. *IEEE Wirel. Commun.* **2018**, *25*, 21–27. [CrossRef]
77. Nguyen, D.C.; N Pathirana, P.; Ding, M.; Seneviratne, A. Blockchain for 5G and Beyond Networks: A State of the Art Survey. *arXiv* **2019**, arXiv:1912.05062
78. Bajracharya, R.; Shrestha, R.; Kim, S.W. An admission control mechanism for 5G LWA. *Sustainability* **2018**, *10*, 1999. [CrossRef]

79. Ortega, V.; Bouchmal, F.; Monserrat, J.F. Trusted 5G Vehicular Networks: Blockchains and Content-Centric Networking. *IEEE Veh. Technol. Mag.* **2018**, *13*, 121–127. [CrossRef]
80. Rahmadika, S.; Lee, K.; Rhee, K. Blockchain-Enabled 5G Autonomous Vehicular Networks. In Proceedings of the 2019 International Conference on Sustainable Engineering and Creative Computing (ICSECC), Bandung, Indonesia, 20–22 August 2019; pp. 275–280. [CrossRef]
81. Aujla, G.S.; Singh, A.; Singh, M.; Sharma, S.; Kumar, N.; Choo, K.R. BloCkEd: Blockchain-Based Secure Data Processing Framework in Edge Envisioned V2X Environment. *IEEE Trans. Veh. Technol.* **2020**, *69*, 5850–5863. [CrossRef]
82. Cebe, M.; Erdin, E.; Akkaya, K.; Aksu, H.; Uluagac, S. Block4Forensic: An Integrated Lightweight Blockchain Framework for Forensics Applications of Connected Vehicles. *IEEE Commun. Mag.* **2018**, *56*, 50–57. [CrossRef]
83. Singh, M.; Kim, S. Blockchain Based Intelligent Vehicle Data sharing Framework. *arXiv* **2017**, arXiv:1708.09721.
84. Liu, M.; Yu, F.R.; Teng, Y.; Leung, V.C.M.; Song, M. Computation Offloading and Content Caching in Wireless Blockchain Networks With Mobile Edge Computing. *IEEE Trans. Veh. Technol.* **2018**, *67*, 11008–11021. [CrossRef]
85. Dai, Y.; Xu, D.; Zhang, K.; Maharjan, S.; Zhang, Y. Deep Reinforcement Learning and Permissioned Blockchain for Content Caching in Vehicular Edge Computing and Networks. *IEEE Trans. Veh. Technol.* **2020**, *69*, 4312–4324. [CrossRef]
86. Iqbal, S.; Malik, A.W.; Rahman, A.U.; Noor, R.M. Blockchain-Based Reputation Management for Task Offloading in Micro-Level Vehicular Fog Network. *IEEE Access* **2020**, *8*, 52968–52980. [CrossRef]
87. Mukherjee, M.; Matam, R.; Shu, L.; Maglaras, L.; Ferrag, M.A.; Choudhury, N.; Kumar, V. Security and Privacy in Fog Computing: Challenges. *IEEE Access* **2017**, *5*, 19293–19304. [CrossRef]
88. Dai, Y.; Xu, D.; Maharjan, S.; Chen, Z.; He, Q.; Zhang, Y. Blockchain and Deep Reinforcement Learning Empowered Intelligent 5G Beyond. *IEEE Netw.* **2019**, *33*, 10–17. [CrossRef]
89. Wang, W.; Hoang, D.T.; Hu, P.; Xiong, Z.; Niyato, D.; Wang, P.; Wen, Y.; Kim, D.I. A Survey on Consensus Mechanisms and Mining Strategy Management in Blockchain Networks. *IEEE Access* **2019**, *7*, 22328–22370. [CrossRef]
90. Kim, S.; Kwon, Y.; Cho, S. A Survey of Scalability Solutions on Blockchain. In Proceedings of the 9th International Conference on Information and Communication Technology Convergence: ICT Convergence Powered by Smart Intelligence, ICTC 2018, Jeju, Korea, 17–19 October 2018; pp. 1204–1207. [CrossRef]
91. Xie, J.; Yu, F.R.; Huang, T.; Xie, R.; Liu, J.; Liu, Y. A Survey on the Scalability of Blockchain Systems. *IEEE Netw.* **2019**, *33*, 166–173. [CrossRef]
92. Sanka, A.I.; Cheung, R.C.C. Efficient High Performance FPGA based NoSQL Caching System for Blockchain Scalability and Throughput Improvement. In Proceedings of the 2018 26th International Conference on Systems Engineering (ICSEng), Sydney, Australia, 18–20 December 2018; pp. 1–8. [CrossRef]
93. Hazari, S.S.; Mahmoud, Q.H. A Parallel Proof of Work to Improve Transaction Speed and Scalability in Blockchain Systems. In Proceedings of the 2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC), Las Vegas, NV, USA, 7–9 January 2019; pp. 916–921. [CrossRef]
94. Xiong, W.; Xiong, L. Smart Contract Based Data Trading Mode Using Blockchain and Machine Learning. *IEEE Access* **2019**, *7*, 102331–102344. [CrossRef]
95. Ali, S.; Wang, G.; White, B.; Cottrell, R.L. A Blockchain-Based Decentralized Data Storage and Access Framework for PingER. In Proceedings of the 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, 1–3 August 2018; pp. 1303–1308. [CrossRef]
96. Petrillo, A.; Pescapé, A.; Santini, S. A collaborative approach for improving the security of vehicular scenarios: The case of platooning. *Comput. Commun.* **2018**, *122*, 59–75. [CrossRef]
97. Petrillo, A.; Pescapé, A.; Santini, S. A Secure Adaptive Control for Cooperative Driving of Autonomous Connected Vehicles in the Presence of Heterogeneous Communication Delays and Cyberattacks. *IEEE Trans. Cybern.* **2020**, 1–16. [CrossRef] [PubMed]
98. Li, X.; Jiang, P.; Chen, T.; Luo, X.; Wen, Q. A survey on the security of blockchain systems. *Future Gener. Comput. Syst.* **2020**, *107*, 841–853 doi:10.1016/j.future.2017.08.020. [CrossRef]
99. Möser, M.; Soska, K. An empirical analysis of linkability in the monero blockchain. *arXiv* **2017**, arXiv:1704.04299.

100. Luu, L.; Velner, Y.; Teutsch, J.; Saxena, P. Smartpool: Practical Decentralized Pooled Mining. In Proceedings of the 26th USENIX Security Symposium, Vancouver, BC, Canada, 16–18 August, 2017; pp. 1409–1426.
101. Cheng, R.; Zhang, F.; Kos, J.; He, W.; Hynes, N.; Johnson, N.; Juels, A.; Miller, A.; Song, D. Ekiden: A Platform for Confidentiality-Preserving, Trustworthy, and Performant Smart Contracts. In Proceedings of the 2019 IEEE European Symposium on Security and Privacy (EuroS&P), Stockholm, Sweden, 17–19 June 2019; pp. 185–200. [CrossRef]
102. Tsankov, P.; Dan, A.; Drachsler-Cohen, D.; Gervais, A.; Bünzli, F.; Vechev, M. *Securify: Practical Security Analysis of Smart Contracts*; Association for Computing Machinery: New York, NY, USA, 2018; pp. 67–82. [CrossRef]
103. Yu, F.R. "vDLT: A Service-Oriented Blockchain System with Virtualization and Decoupled Management/Control and Execution. *arXiv* **2018**, arXiv:1809.00290.
104. Dorri, A.; Kanhere, S.S.; Jurdak, R.; Gauravaram, P. Blockchain for IoT security and privacy: The case study of a smart home. In Proceedings of the 2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops), Kona, HI, USA, 13–17 March 2017; pp. 618–623. [CrossRef]
105. Kim, T.; Noh, J.; Cho, S. SCC: Storage Compression Consensus for Blockchain in Lightweight IoT Network. In Proceedings of the 2019 IEEE International Conference on Consumer Electronics (ICCE), Las Vegas, NV, USA, 11–13 January 2019; pp. 1–4. [CrossRef]
106. Liu, Y.; Wang, K.; Lin, Y.; Xu, W. LightChain:A Lightweight Blockchain System for Industrial Internet of Things. *IEEE Trans. Ind. Inform.* **2019**, *15*, 3571–3581. [CrossRef]
107. Zaman, M.U.; Shen, T.; Min, M. Proof of Sincerity: A New Lightweight Consensus Approach for Mobile Blockchains. In Proceedings of the 2019 16th IEEE Annual Consumer Communications & Networking Conference (CCNC), Las Vegas, NV, USA, 11–14 January 2019; pp. 1–4. [CrossRef]
108. Shen, H.; Zhou, J.; Cao, Z.; Dong, X.; Choo, K.R. Blockchain-based Lightweight Certificate Authority for Efficient Privacy-preserving Location-Based Service in Vehicular Social Networks. *IEEE Internet Things J.* **2020**, *7*, 6610–6622. [CrossRef]
109. Xiong, Z.; Feng, S.; Niyato, D.; Wang, P.; Han, Z. Optimal Pricing-Based Edge Computing Resource Management in Mobile Blockchain. In Proceedings of the 2018 IEEE International Conference on Communications (ICC), Kansas City, MO, USA, 20–24 May 2018; pp. 1–6. [CrossRef]
110. Qiu, C.; Yao, H.; Jiang, C.; Guo, S.; Xu, F. Cloud Computing Assisted Blockchain-Enabled Internet of Things. *IEEE Trans. Cloud Comput.* **2019**, 1. [CrossRef]
111. Sharma, P.K.; Singh, S.; Jeong, Y.S.; Park, J.H. DistBlockNet: A Distributed Blockchains-Based Secure SDN Architecture for IoT Networks. *IEEE Commun. Mag.* **2017**, *55*, 78–85. [CrossRef]
112. Mishra, A.D.; Singh, Y.B. Big data analytics for security and privacy challenges. In Proceedings of the 2016 International Conference on Computing, Communication and Automation (ICCCA), Noida, India, 29–30 April 2016; pp. 50–53. [CrossRef]
113. Sultan, K.; Ali, H.; Zhang, Z. Big Data Perspective and Challenges in next Generation Networks. *Future Internet* **2018**, *10*, 56. [CrossRef]
114. Karafiloski, E.; Mishev, A. Blockchain solutions for big data challenges: A literature review. In Proceedings of the IEEE EUROCON 2017—17th International Conference on Smart Technologies, Ohrid, Macedonia, 6–8 July 2017; pp. 763–768. [CrossRef]
115. Uchibeke, U.U.; Schneider, K.A.; Kassani, S.H.; Deters, R. Blockchain Access Control Ecosystem for Big Data Security. In Proceedings of the 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), Halifax, NS, Canada, 30 July–3 August 2018; pp. 1373–1378. [CrossRef]
116. Lampropoulos, K.; Georgakakos, G.; Ioannidis, S. Using Blockchains to Enable Big Data Analysis of Private Information. In Proceedings of the 2019 IEEE 24th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD), Limassol, Cyprus, 11–13 September 2019; pp. 1–6. [CrossRef]
117. Saad, W.; Bennis, M.; Chen, M. A Vision of 6G Wireless Systems: Applications, Trends, Technologies, and Open Research Problems. *IEEE Netw.* **2020**, *34*, 134–142. [CrossRef]

118. Chowdhury, M.Z.; Shahjalal, M.; Ahmed, S.; Jang, Y.M. 6G Wireless Communication Systems: Applications, Requirements, Technologies, Challenges, and Research Directions. *arXiv* **2019**, arXiv:1909.11315.
119. Yaacoub, E.; Alouini, M.S. A Key 6G Challenge and Opportunity—Connecting the Remaining 4 Billions: A Survey on Rural Connectivity. *arXiv* **2019**, arXiv:1906.11541.
120. Tiba, K.; Choo, K.K.R.; Parizi, R.M.; Zhang, Q.; Dehghantanha, A.; Karimipour, H.; Choo, K.K.R. Secure Blockchain-Based Traffic Load Balancing Using Edge Computing and Reinforcement Learning. In *Blockchain Cybersecurity, Trust and Privacy. Advances in Information Security*; Dehghantanha, A., Reza, M.; Ed.; Springer Nature: Geneva, Switzerland, 2020; Volume 79, pp. 99–128. [CrossRef]