sensors

MDPI

Review

Blockchain-Based Authentication in Internet of Vehicles: A Survey

Sohail Abbas [1], Manar Abu Talib [1], Afaf Ahmed [2], Faheem Khan [3], Shabir Ahmad [4] and Do-Hyeun Kim [5,*]

[1] Department of Computer Science, College of Computing and Informatics, University of Sharjah, Sharjah 27272, United Arab Emirates; sabbas@sharjah.ac.ae (S.A.); mtalib@sharjah.ac.ae (M.A.T.)
[2] College of Engineering, Al Ain University, Al Ain 64141, United Arab Emirates; afaf.ahmed@aau.ac.ae
[3] Department of Computer Engineering, Gachon University, Seongnam-si 13120, Korea; faheem@gachon.ac.kr
[4] Department of IT Convergence Engineering, Gachon University, Seongnam-si 13120, Korea; shabir@gachon.ac.kr
[5] Department of Computer Engineering, Jeju National University, Jeju 63243, Korea
* Correspondence: kimdh@jejunu.ac.kr

Abstract: Internet of Vehicles (IoV) has emerged as an advancement over the traditional Vehicular Ad-hoc Networks (VANETs) towards achieving a more efficient intelligent transportation system that is capable of providing various intelligent services and supporting different applications for the drivers and passengers on roads. In order for the IoV and VANETs environments to be able to offer such beneficial road services, huge amounts of data are generated and exchanged among the different communicated entities in these vehicular networks wirelessly via open channels, which could attract the adversaries and threaten the network with several possible types of security attacks. In this survey, we target the authentication part of the security system while highlighting the efficiency of blockchains in the IoV and VANETs environments. First, a detailed background on IoV and blockchain is provided, followed by a wide range of security requirements, challenges, and possible attacks in vehicular networks. Then, a more focused review is provided on the recent blockchain-based authentication schemes in IoV and VANETs with a detailed comparative study in terms of techniques used, network models, evaluation tools, and attacks counteracted. Lastly, some future challenges for IoV security are discussed that are necessary to be addressed in the upcoming research.

Keywords: authentication; blockchain; Internet of Vehicles; Vehicular Ad-hoc Networks

Citation: Abbas, S.; Talib, M.A.; Ahmed, A.; Khan, F.; Ahmad, S.; Kim, D.-H. Blockchain-Based Authentication in Internet of Vehicles: A Survey. *Sensors* **2021**, *21*, 7927. https://doi.org/10.3390/s21237927

Academic Editor: Rongxing Lu

Received: 28 October 2021
Accepted: 22 November 2021
Published: 27 November 2021

1. Introduction

With the huge increase in the number of vehicles on roads nowadays, more accidents and traffic congestion issues are encountered. This raises the need for serious arrangements to ensure roads' safety and traffic efficiency. Different technologies have been introduced towards maintaining safer and time-efficient driving on roads, such as, Vehicular Ad-hoc Networks (VANETs) in which the vehicles exchange data about their speed, location, etc., and other road-related information to raise their awareness about surrounding road conditions and help them making better and effective decisions. However, with the rapid advancement in today's technologies such as ubiquitous connectivity, wireless technologies, sensor devices, smart vehicles, and cloud computing platforms, the need for more powerful vehicular networks has increased. Hence, the IoV has appeared that can exploit and incorporate all these advanced technologies in order to provide more satisfying real-time services for vehicles' drivers and passengers.

IoV has emerged with great potential to support various services and offer several benefits to the transportation system such as cost effectiveness, time efficiency, road safety [1], traffic management [2–4], evolution of smart cities [5,6], autonomous driving [7–10] alarms and dynamic warning systems [11–13] as well as recording fatal occurrences [14]. However, in order for the IoV system to be able to secure such services, enormous amounts of data

need to be generated and exchanged among the different IoV entities including vehicles, pedestrians, and roadside infrastructure. Since this information exchange takes place through an open-channel wireless network, the exchanged messages are vulnerable to various security attacks that could undermine the privacy of the communicating entities and the confidentiality of their data via eavesdropping or even affect the integrity of the transmitted messages by tampering them before reaching their target destination. Other types of security attacks that could be encountered in IoV environments are the attacks that target the authenticity of users. Here, a malicious entity masquerades a legitimate user and may commit malicious activities in the network. Therefore, efficient authentication is necessary to prevent such attacks in IoV.

On the other hand, blockchain technology has recently drawn the attention of both industry and academia due to its efficient characteristics represented in decentralization, immutability, consensus, fault tolerance, and enhanced security. Blockchain was first known as the enabling technology behind Bitcoin or cryptocurrency. Yet, it has recently attracted various emerging domains such as smart cities [15–17], smart grids [18–20], Internet of Things (IoT) [21,22], Cyber Physical Systems (CPS) [23–25], robotics [26,27], machine learning [28,29], and health systems [30–32]. IoV platforms have also started to adopt blockchain for various services which include data management [33,34], resource trading [35,36], resource sharing [37,38], vehicle management [39,40], ride sharing [41,42], traffic control [43,44], and forensics applications [45,46]. In this paper, we highlight the use of blockchain in IoV and VANETs for authentication by surveying a number of recent blockchain-based authentication schemes.

Numerous surveys have recently been published discussing the authentication approaches and protocols in the vehicular networks of VANETs and IoV which are summarized in Table 1. Some of the surveys have focused on authentication in IoV and/or VANETs as part of the Intelligent Transportation Systems (ITS) whereas others have exhibited wider perspective by discussing IoV authentication as a subsection of the Internet of Things (IoT) technology.

Table 1. Comparison of recent surveys on authentication in IoV and VANETs networks.

Ref.	Year	Target Area	VANETs to IoV Transition	Security Attacks and/or Requirements	Blockchain-Based Authentication	Features
[47]	2017	IoT	X	√	X	• Discusses symmetric and asymmetric cryptographic-based authentication protocols. • Covers authentication protocols in a wide range of IoT environments, namely, IoV, IoS, IoE, and M2M. • Presents threat models, countermeasures and formal security verification techniques used by the surveyed papers.
[48]	2017	VANETs	X	√	X	• Surveys a range of authentication schemes that are based on cryptography, digital signature, and message verification. • Provides a performance comparison in terms of communication and computation overheads.

Table 1. *Cont.*

Ref.	Year	Target Area	VANETs to IoV Transition	Security Attacks and/or Requirements	Blockchain-Based Authentication	Features
[49]	2019	IoT	X	√	X	• Provides a multi-criteria classification for the surveyed authentication schemes which includes authentication factor, procedure, and architecture, IoT layer, use of tokens and use of hardware. • Presents different security requirements and issues faced by each IoT layer.
[50]	2019	VANETs	X	√	X	• Discusses authentication and privacy schemes in VANETs while providing a good taxonomy based on the privacy preserving technique used. • Presents the security of each scheme in terms of security requirements and their corresponding attacks. • Shows performance efficiency w.r.t computational cost and communicational cost for each scheme.
[51]	2020	VANETs	X	X	X	• Addresses authentication, privacy, and secure message dissemination in VANETs. • Proposes multi-categorization based on the tools and techniques used in the surveyed papers.
[52]	2020	IoV	√	√	X	• Provides a good taxonomy of various security protocols in IoV. • Surveys authentication protocols in IoV. • Discusses security aspects: threats and attacks in IoV. • Provides a performance comparison in terms of communication and computation overheads.
[53]	2020	IoV	√	X	√	• Provides a comprehensive comparison of the blockchain-based applications in vehicular networks. • Analyzes the requirements of the blockchain-based applications in vehicular networks. • Discusses a range of challenges related to the integration of blockchain within vehicular networks.

Table 1. *Cont.*

Ref.	Year	Target Area	VANETs to IoV Transition	Security Attacks and/or Requirements	Blockchain-Based Authentication	Features
[54]	2021	IoV	√	X	X	• Provides seven different aspects for combining the blockchain technology with IoV while briefly surveying some schemes for each of these aspects. • Overviews some research directions in the field of blockchain-enabled IoV.
[55]	2021	IoV	X	√	√	• Provides a detailed review on various existing blockchain techniques for IoV security. • Provides a good categorization for the existing blockchain-based IoV security methods. • Presents a clear analysis for the surveyed blockchain-based IoV security schemes in terms of techniques, tools, and performance metrics. • Discusses a couple of future research aspects.
Our survey	2021	VANETs and IoV	√	√	√	• Covers the specific area of VANETs and IoV, which provides a more focused reference for researchers in the field of IoV, meanwhile a more comprehensive reference in vehicular technology and ITS. • Highlights the efficiency of blockchain in IoV by discussing blockchain-based authentication schemes. • Provides a clear taxonomy in terms of the type of blockchain used for authentication. • Presents a detailed comparison between the surveyed papers in terms of techniques used, attacks counteracted, network models, and evaluation tools. • Discusses whether each authentication scheme supports privacy preservation of user identity or not. • Focuses on the attacks on authentication, their targeted OSI layers, and possible remedies.

In order to highlight the contribution of this paper, a number of recent state-of-art surveys are summarized and compared in Table 1. In [47], the cryptographic-based authentication protocols have been discussed in a wide range of IoT environments, namely, IoV, Internet of Sensors (IoS), Internet of Energy (IoE), and Machine to Machine Communication (M2M). In [48], a range of authentication schemes that are based on cryptography, digital signature, and message verification in the context of VANETs have been presented.

IoV authentication has been implicitly reviewed in [49] by introducing a multi-criteria classification for the authentication schemes in the IoT environment in general. A broad range of crypto-based authentication schemes in VANETs environments [50,51] and IoV networks [52] have also been reviewed. However, despite discussing the authentication protocols from different points of view and introducing diverse categorization criteria, all the above surveys have the common factor of reviewing the cryptographic-based authentication schemes in IoV or VANETs and none of them has reviewed the authentication schemes that are based on blockchains.

On the other hand, blockchain-based applications in IoV have been addressed by many surveys recently. For instance, the authors in [53] have surveyed a number of blockchain-based applications that aim to improve the security, privacy, trust and cooperation in IoV networks. Seven different aspects where blockchain technology can be incorporated with IoV have been discussed in [54] such as IoV security, trust management, and data management. Moreover, different blockchain-based IoV security methods have been categorized and reviewed in [55]. Although these surveys might have mentioned a few blockchain-based authentication schemes in IoV, they have briefly mentioned them on the run as a small part of the broad field of IoV security and none of them has provided a detailed survey that is only dedicated to the blockchain-based authentication schemes in IoV. Thus, the main contributions of this survey are:

- Highlighting the significance of the blockchain technology in IoV and VANETs by presenting a wide range of the blockchain-based authentication schemes that are proposed in the recent literature.
- Providing the first detailed survey focusing on the application of blockchain technology to a specific aspect of IoV security; that is, the authentication. Considering both IoV and VANETs technologies when surveying the different blockchain-based authentication schemes instead of restricting them to only one vehicular technology, which can provide a comprehensive source for researchers interested in the field of blockchain-based authentication.

The organization of the paper is as follows: Section 2 presents some preliminary information related to IoV and blockchain. Then, the security requirements and challenges along with some common security attacks and threats that can be encountered in IoV and VANETs paradigms are discussed in Section 3. After that, the main part of the paper is represented by Sections 4 and 5 where a wide range of blockchain-based authentication schemes in IoV and VANETs are reviewed and compared. Section 6 then suggests some future research challenges after which the paper is finally concluded in Section 7.

2. Background

2.1. Internet of Vehicles

IoV is an emerging field that mainly incorporates ITS and IoT technologies, while covering a wide range of other technologies and applications such as vehicular information services, advanced wireless communication technologies, cloud computing, edge computing, and automotive electronics to provide intelligent transportation services and enhance the quality of roads. It integrates the intelligent in-vehicle sensor devices with the intra-vehicle and inter-vehicle wireless communication technologies along with Internet technology to collect and exchange vehicle-related and traffic-related data that can be later used for making better road-related actions and decisions. IoV consists of three basic components: (1) the intra-vehicular network, (2) inter-vehicular network, and (3) vehicular mobile Internet [56]. This includes the communication between vehicles in the same vehicular network, the communication between different vehicular networks, and the connection between vehicles and mobiles, respectively. The functionality of IoV imposes equipping vehicles with several smart units and devices including electronic control units, On Board Units (OBUs), sensors, event data records, cameras, GPS modules as well as a diverse number of wired (Controller Area Network and Local Interconnect Network buses) and wireless (i.e., Bluetooth) communication technologies.

The former technology to IoV is the VANETS which was basically introduced to improve the traffic efficiency and road safety by establishing connectivity and exchanging information between the moving vehicles with and without the aid of any pre-established roadside infrastructure via different communication modes namely, Wireless Access in Vehicular Environments (WAVE) based Wi-Fi, ad-hoc, and hybrid. Despite its efficiency in addressing road safety and traffic management issues with low operational cost, VANETs exhibit some commercialization problems which include but are not limited to the following [57]:

1. VANETs' framework could not fully support the global and sustainable services targeted by ITS applications. This is caused by the pure ad-hoc communication architecture, in which an on-road vehicle can lose its granted services once it disconnects from an ad-hoc network. This is due to the inability of collaborating with other alternative reachable networks.
2. Internet connectivity in VANETS could not be ensured, which affects the availability of commercial applications for vehicles' drivers and passengers since those applications rely on reliable Internet connectivity.
3. Despite the rapid technological advancement of personal mobile devices, they could not communicate with VANETs due to the incompatible network architecture.
4. Intelligent decision making, and big data analytics applications were not possible in certain VANETs architectures. This could be related to the computing and storage constraints and the lack of cloud computing services.
5. The application services could not guarantee high level of accuracy, since VANETs localize the computation and processing of traffic data information.

The above limitations of VANETs have drawn the attention of researchers and industrial developers to extend the capabilities of the existing vehicular networks to move further steps towards providing more efficient vehicular services and achieving the global objectives of ITS. Consequently, IoV has emerged as an advanced vehicular technology that attempts to overcome the shortcomings of conventional VANETs through supporting a high range of mobility, strong connectivity among vehicles and with roadside infrastructure, reliable Internet connection, and high interactivity with personal devices. IoV can also provide an immediate management of risk situations through maintaining low delay and delivering high reliability and robustness. Cloud and edge computing capabilities, processing, and analysis of collected data to transform them into useful information through big data analytics tools to provide services to consumers and businesses are as well positive points for the IoV.

In addition, IoV has brought the ability to support diverse types of interaction models including Vehicle-to-Vehicle (V2V), Vehicle-to-Roadside-unit (V2R), Vehicle-to-Infrastructure (V2I), Vehicle-to-Pedestrian (V2P), Vehicle-to-Sensor (V2S), and many others as indicated in Figure 1. V2V and V2R indicate the interaction among the vehicles and the interaction between the vehicles and the RSUs, respectively, via wireless protocols such as WAVE. V2I is the communication between vehicles and infrastructure possibly via Wi-Fi, Long Term Evolution (LTE), or 5G. While V2S represents the onboard sensor communication via Ethernet and Wi-Fi, V2P refers to the communication among vehicles and personal devices such as smartphones via Apple's CarPlay, Open Automotive Alliance Android system, or Near Field Communication [58,59].

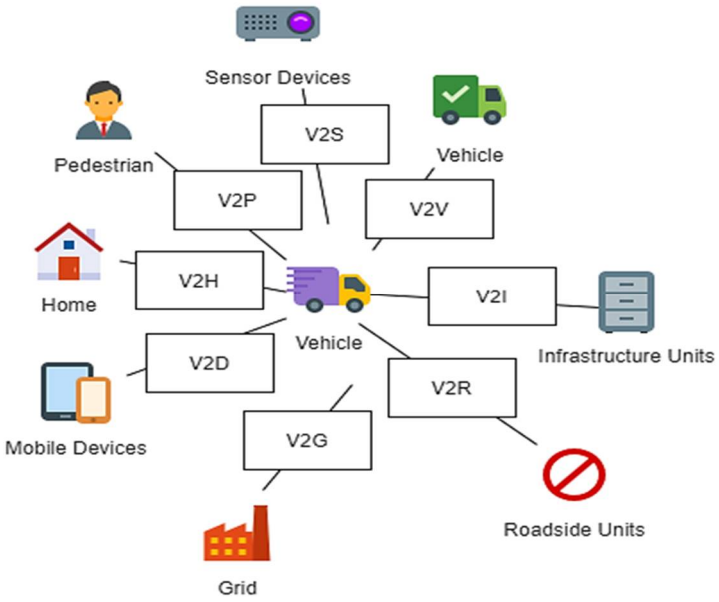

Figure 1. Communication models in IoV.

Different layered architectures for IoV frameworks have been proposed in the literature, which differ in the number and/or names of layers proposed. These architectures compete to optimize the number of layers and to enhance the distinguishability between the different layers [57,58,60–63]. The most common IoV architecture can be seen in Figure 2 which defines six layers, namely, physical, communication, processing, services, business, and security. The main responsibility of the physical layer is to gather information about vehicles and their surrounding environment such as vehicle's speed, position, travelling direction, on-road vehicular density, weather conditions, and others through the sensing devices, actuators, GPS modules, and access points installed on the vehicles. RSUs and other personal devices may also be used. The collected data are then transferred in a secure way to the processing layer through the communication layer, which employs diverse wireless communication standards and network modules to guarantee interoperability between the different heterogeneous network entities such as WAVE, WiFi, RFID, Bluetooth, 4G/LTE, UW, and satellites. The processing layer represents the storage, processing, and transformation of the data received from the lower layers into useful information to be used for decision making. This includes the adoption of various big data analytics tools and cloud computing platforms. The services layer then takes the information processed and the decisions made by the processing layer and employs them to provide intelligent IoV services and applications to the end users which can contribute to road safety and traffic efficiency. The business layer's responsibilities can include decisions related to economics investment, budget estimation and regulation, pricing, and operations management. Finally, the security layer concerns about secure and reliable data collection and communication among the different nodes to prevent against diverse number of security attacks and threats that can be encountered in IoV environments. Since security is the main theme of this paper, we will discuss more on this in the coming sections.

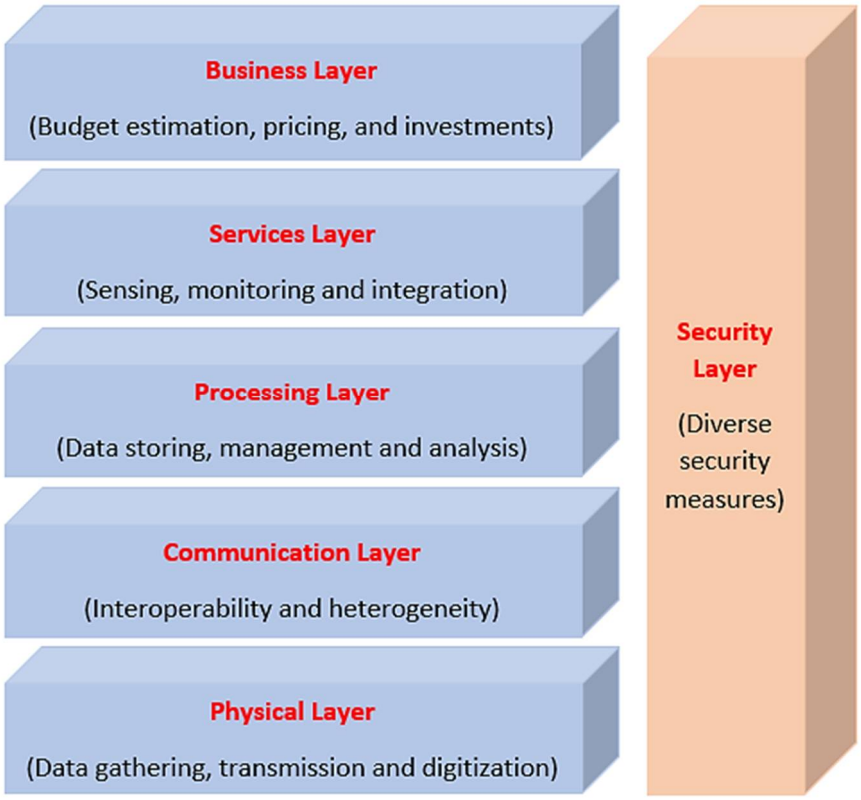

Figure 2. The proposed six-layers architecture of IoV.

2.2. Blockchain

A blockchain, also called a Distributed Ledger Technology (DLT), can be defined as a group of connected blocks used to store transactions' records or events and is maintained by all the participating users distributed over the network. Blockchain technology removes the reliance on a central authority, since it allows all users to generate and validate transactions directly in a peer-to-peer network which helps significantly in reducing the financial and time related costs associated with the intermediate party. Building the blocks of a blockchain relies on two key technologies, namely, cryptography [64–66] and consensus mechanisms [67–69].

Cryptography is adopted in blockchain to ensure the security and privacy of the data and the anonymity of the participants thereby using cryptographic hash functions and digital signatures [70]. The adoption of cryptographic hash function is quite popular in blockchains, where each block is linked to the previous block (its parent block) by keeping the hash value of the previous block in its own header, except the genesis block, i.e., the first block in the chain. The first block has no parent block and thus the hash value of the previous block is set to zero. This hash-based linking structure makes the blockchain immutable due to the uniqueness of the hash values used. The digital signature, on the other hand, is a type of asymmetric cryptography where each user owns a pair of public and private keys. The typical digital signature algorithm used in most blockchain applications is the Elliptic Curve Digital Signature Algorithm (ECDSA).

Consensus mechanisms are used in the blockchain to establish trust in an untrustworthy environment and to verify the correctness and integrity of the transactions data being added to the public ledger. Blockchain consensus can be defined as "the agreement of a common value among a group of nodes in blockchain systems" [71]. Several consensus mechanisms have been proposed in different blockchain scenarios which differ in their fault tolerance, scalability, power consumption, and application-dependent scenarios. However, they all agree to provide consistency and transparency to the data blocks. Two broad categories of blockchain consensus protocols are suggested in [67], namely, probabilistic-finality

consensus and absolute-finality consensus protocols. The former can only guarantee an eventual consistency whereas the latter ensures a strong consistency. Some of the most common consensus protocols are Proof of Stack (PoS), Proof of Work (PoW), and Practical Byzantine Fault Tolerance (PBFT). However, other less common consensus mechanisms also exist in blockchain applications such as Leased Proof of Stack [72], Proof of Elapsed Time [73], Proof of Activity [74], Proof of Importance [75], Proof of Capacity [76], Proof of Burn [77], and Proof of Vote [78].

Three types of blockchains are commonly defined and agreed upon by most of the literature, namely, public blockchain, private blockchain, and consortium blockchain. The different types are distinguished from each other by their consensus making, read permission, immutability, and degree of centralization [68]. Public blockchain is a non-restrictive, permissionless distributed ledger in which everyone can access and validate the transactions and participate in running the consensus mechanism. Public blockchains are completely decentralized and are suitable for fully opened systems where untrusted entities may join the network. Typical examples of public blockchains include Bitcoin, Ethereum, and Litecoin [69,79–81]. On the other hand, Private blockchain is a restrictive, permissioned blockchain in which only a sub-group of predefined nodes can maintain and validate the ledger. A private blockchain is fully controlled by a single organization, thus it can be regarded as a centralized network. Private blockchains are suitable for closed systems where all nodes fully trust each other. Consortium blockchain is a partially decentralized ledger managed by several organizations in which only a small group of nodes is pre-selected to perform the consensus. It is suitable for semi-closed systems consisting of few enterprises and thus is normally found in the banking sector and other governmental organizations. Consortium blockchains are regarded as a combination of both public and private blockchains. Typical examples are Stellar [71], R3CEV [79], Hyperledger [82], and Ripple [83].

However, other blockchain classifications have been suggested in the relevant literature. For instance, the authors in [69] have divided blockchains into four types: public, private, consortium, as well as hybrid. Similarly, two blockchain categories, permissioned and permissionless blockchains, are proposed in [84].

2.3. Motivations to Use Blockchain in IoV

IoV is a large-scale and heterogenous network that combines a large number of connected vehicles, roadside infrastructure, mobile personal devices, central and distributed storage, and computation servers in case of incorporating cloud and edge computing platforms. This along with the open-channel wireless communication model and the public Internet connectivity that dominate most of the communication makes the IoV network vulnerable to a variety of security attacks that could threaten the applications of IoV such as navigation, accident detection and notification, dynamic alternative routing, route optimization, and congestion management which consequently constitutes a threat and danger on drivers and passengers on the road. Furthermore, since IoV scenarios include high mobility and exchange of huge amount of data as well as requiring real-time services and decision making, more efficient, powerful, and reliable technologies must be adopted in IoV frameworks in place of the conventional techniques.

On the other hand, blockchain technology has emerged recently as a decentralized storage mechanism in various industry applications due to its strong capabilities not only in distributed storage aspect, but also in terms of security, privacy, performance, automation, and reduced computational cost. Recently, blockchain has also been brought to the IoV paradigm to serve different purposes such as data protection and management, resource trading, resource sharing, ride sharing, traffic control and management, and forensic applications.

The various features a blockchain can provide have motivated researchers and the industry to incorporate blockchain technology into the IoV. These properties include the following [85,86]:

1. Decentralization: Unlike the centralized-storage platforms where both data storage and management are handled by a trusted centralized node, blockchain technology exhibits a decentralized nature in which data records are kept and managed by all participating entities. This reduces the resource bottlenecks issue and maintenance cost associated with the centralized sever arrangements and avoids the single point of failure issue which all can be beneficial for IoV environments.
2. Immutability: Since the creation and validation of new blocks of transactions should be agreed upon by all or most of the peers via the different consensus mechanisms before being added to the blockchain, the blockchain is almost impossible to be tampered with or modified.
3. Security and privacy: The cryptographic nature of blockchain where both cryptographic hash functions and digital signatures are adopted can ensure the security of transactions data and the privacy of the participating users in IoV.
4. Transparency: Since all participants keep a replica of the public ledger, they can access all the timestamped blockchain transactions. This enables the peers to manage, look up and verify transactions at any time in a transparent manner without an intermediary. This self-auditability and transparency not only promote the relief of the peers by managing their own transactions, but also mitigates the time and financial costs associated with the intermediate party.
5. Automation: Blockchain technology supports the adoption of smart contracts which are software scripts that can be executed automatically by a triggering event or upon meeting some pre-defined set of rules. This automation property of blockchain can enhance the efficiency of many IoV applications and help provide various services autonomously without a need for a trusted entity.
6. Traceability: Each transaction record is kept in the blockchain with a timestamp indicating its time of occurrence and joining the public ledger. This timestamped recording nature helps identifying the events in a chronological order which enhances the traceability and can support the non-repudiation requirement in IoV.

3. Security Issues in IoV and VANETs

IoV and VANETs have various features that are advantageous to vehicles' drivers and passengers, pedestrians as well as the whole industrial business. However, like any new-emerging technology, IoV and VANETs come with several risks and security threats. The continuous mobility of vehicles, the existence of a third party acting as an authority to certify the nodes, and the wireless mode of communication among the different nodes make these vehicular networks vulnerable to wide range of security threats and attacks. Identifying the different security requirements and exploring the possible attacks that threaten these vehicular frameworks is the first step towards resisting them. Accordingly, in this section we first present the different security requirements and challenges for vehicular networks in Section 3.1 followed by a wide range of security attacks in Section 3.2.

3.1. Security Requirements and Challenges in Vehicular Networks

The IoV networks are an amalgamation of diverse technologies with different standards and regulations (such as Internet connections, different wireless technologies, sensors, cloud services); which make IoV vulnerable to various types of security attacks. Depending upon the attacker objective(s), the attack launched might be passive or active, generated internally or from an external source. However, regardless of the attack's source or activity type, these security threats are commonly classified into different categories based on the security aspect(s) of the network being compromised. For example, an attack could affect the authenticity of the users, the integrity of IoV data, or the availability of the provided services.

Guided by the various security threats an IoV system can suffer from, different security aspects have been defined in the literature. These security aspects can be classified into: (1) Security requirements that an efficient IoV system should maintain and (2) Security

challenges that face any security subsystem of an IoV environment. Figure 3 illustrates these security requirements and challenges. Following are the different security requirements of an IoV system [87–91]:

1. Authentication: It means ensuring that the received data is generated by a legitimate sender, or in other words, making sure that the entity that sent the data must be the true actual entity it claims to be. It guarantees that the entities involved in the communication are authentic, not masqueraded by some attacker who forwards the messages on their behalf. Sybil attack, masquerading attack, impersonation attack, spoofing attack, replay attack, and wormhole attacks are examples of attacks that target the authenticity of IoV users.
2. Availability: It is a basic requirement in IoV environment especially for the real-time critical applications where even a minor delay cannot be tolerated and made the information useless. Therefore, the IoV system should be available all the time to provide real-time information and services to all legitimate users and be able to tolerate partial system faults and failure issues through backups and replications. Moreover, a mature IoV system must have the ability to function under intense network load with the increasing number of participants. The common attacks that target the availability service are the denial-of-service and distributed denial-of-service attacks.
3. Confidentiality: Some IoV applications include sensitive information that are accessed only by certain legitimate users. Therefore, confidentiality of this information must be insured through encryption to prevent it from being revealed and interpreted by any illegal entity even upon eavesdropping.
4. Data integrity: It means there is no distortion—whether intentionally or accidentally—in the received data. In other words, the sent data and the received data are identical. Typical attacks on integrity can be data manipulation attack and malware attack.
5. Non-repudiation: It guarantees that any involved user in the IoV environment cannot deny any of its past activities, i.e., sending or receiving any piece of information. This ensures that an attacker can be identified, and all its communicated messages can be retrieved if needed for subsequent actions.
6. Access control: Each participating entity in the IoV network is assigned different rights and privileges to access the network resources. This security requirement guarantees that each node performs its functions based on the services it is entitled to.
7. Privacy and anonymity: The users' real identities may need to be made hidden using anonymous identities or pseudonyms to protect their privacy. Additionally, some location information such as the driving traces and tracks followed by the vehicles are sometimes preferred to be anonymous in order to prevent unauthorized location tracking.
8. Data verification: Since malicious entities can modify the information sent by the sender, a regular data verification process is usually performed to identify the manipulated or tampered messages and thus reject or drop them (if found) to prevent misleading the receiving entities into taking improper decisions.
9. Real-time guarantee and efficient routing: The majority of IoV and VANETs applications are real-time, such as accidents detection and warnings dissemination, which must be carried out within certain time constraints, otherwise the safety of drivers and passengers could be threatened, and the delayed information will become worthless. To be able to meet these time constraints, efficient secure routing protocols should be adopted to guarantee delivering the packets in their entirety and on time.
10. Traceability and revocability: Despite the need for preserving the privacy of IoV users in general by hiding their real identities, the legal authorities should have the ability to retrieve the vehicles' real identities in case of misbehaving to revoke them as well as in case of disputes.
11. Scalability: With the increasing number of vehicles on the roads nowadays, more vehicles and entities are joining the network. Thus, a good vehicular network should

be able to scale-up accordingly. However, this nodes extension may expose the network to higher security issues if not controlled and monitored properly. Therefore, monitored scalability is another security requirement of the IoV system.

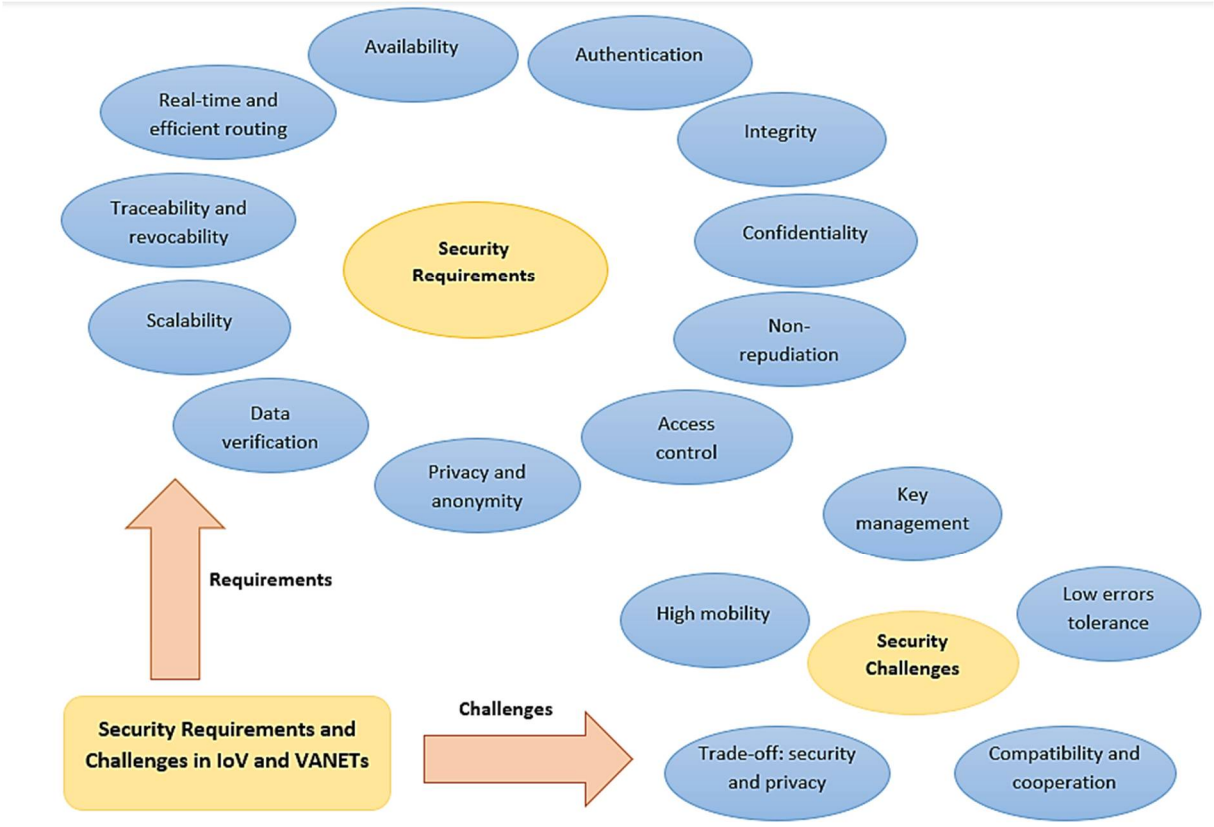

Figure 3. The security requirements and challenges in IoV and VANETs platforms.

The following are different security challenges that might be faced by any IoV paradigm [89,92–97]:

1. High mobility: Data packets must be preserved and kept unmodified during the entire uncertain routing process from the sender to the receiver and should also be delivered on time to satisfy the real-time security requirement. However, the high mobility of nodes in IoV and VANETs networks, and the continuously varying network topology have led to the transient nature of V2V and V2I interactions, which makes the real-time guarantee and non-repudiation security requirements much more difficult.
2. Low errors tolerance: Any minor delay in receiving information or delivering packets in IoV may result in unacceptable situations or even road disasters, thus the time constraints are of high importance in such environments. However, the limited bandwidth and the unstable network quality in IoV caused by the huge number of vehicles being served, their mobility, and the unpredictable changes in wireless networks hinder the real-time security requirement. Therefore, some preventive security measures must be applied so that the drivers can be proactive in case of any emergency situations.
3. Key management: Several authorities and stakeholders are considered important participants in IoV such as governmental institutions and vehicle manufacturers. Hence, it has always been a security challenge to delegate a certain authority among these stakeholders to serve as a fully Trusted Authority (TA) that is responsible for key distribution, management, and revocation, since choosing the wrong authority

without considering its hidden intents and benefits could severely affect the security of the IoV system. Moreover, due to the scale of IoV and VANETs networks, the Certificates Revocation Lists (CRLs) that are responsible for the revocation of misbehaving and malicious vehicles become too long and thus not feasible which raises the overhead of the certificate revocation process. Thus, maintaining a balance between efficient key distribution/revocation process and low overhead is another challenge on IoV security.

4. Tradeoff between security and privacy: In general, the more secure the system is, the less privacy it can provide for users. Many drivers and passengers may not be willing to sacrifice their privacy by sharing their private sensitive data such as their location and destination while caring for security at the same time. Thus, maintaining a good balance between high security and reasonable user privacy is another major security challenge in IoV.
5. Compatibility and cooperation: Due to the divergent interests and targets of the various IoV participating parties such as vehicle manufacturers, consumers, and governmental organizations, it is a big challenge to align their interests properly.

3.2. Security Threats and Attacks in Vehicular Networks

As stated previously, different types of security attacks can be launched against IoV or VANETs, whether passive or active, insider or outsider. However, the common factor of all of them is that they constitute a serious threat to the security of the users, the integrity of the flown data, and consequently the safety of the vehicles' drivers and passengers. Various security attacks and threats in vehicular networks (i.e., IoV and VANETs) have been defined in the literature [89,95,98,99]. Following is some of the most common ones:

- Channel Interference Attack: This is also known as jamming attack, which is the act of interfering with the wireless communication links to hinder and disrupt the quality of communication between connected IoV devices.
- Denial of Service (DoS) Attack: In this attack the attacker floods the IoV network with fake unnecessary requests so that the service provider is no longer able to handle the legitimate requests issued by the genuine users.
- Distributed Denial of Service (DDoS) Attack: It is an advanced type of DoS attack, in which the fake requests are launched from several distributed nodes forming botnets.
- Man-in-the-Middle Attack: In this attack, an attacker places itself in the middle of two communicating legitimate entities to receive the data from the sender and then forward it to the receiver. When the message passes through the attacker, he/she could modify it before forwarding it to the receiver or just reveal its content.
- Message Tampering Attack: This attack aims to corrupt the messages and spread false information in the network by manipulating and fabricating the contents of the communicated messages. This can badly affect the road safety and the services provided by IoV thereby harming passengers and drivers.
- Eavesdropping Attack: It is also referred to as traffic analysis attack, in which the attacker monitors the network to track vehicle routes for some malicious purposes. The attacker eavesdrops on the communication channels to examine the messages flowing in the network.
- Malware Attack: In this attack, the attacker injects malicious software or viruses in the system files to contaminate the network, which can be leveraged to disrupt the network services and/or to manipulate users' data.
- Message Holding Attack: Here, the attacker drops some sensitive messages that hold important data about road conditions that could greatly affect the decision of the drivers on road and thus the road safety is compromised. It also enables the drivers to keep these messages for future use (replaying) in the network.

The above-defined attacks are examples of common security threats that can affect the confidentiality and integrity of IoV data, as well as the availability of the entire IoV system. Table 2 depicts a mapping between the various presented security attacks and the

security requirements affected by each of them. However, since our target in this survey paper is to review and discuss the authentication-related issues in IoV, we dedicate more focus to the attacks and threats that target the authentication domain specifically. Therefore, Table 3 illustrates the authentication attacks with their targeted OSI layer along with some proposed solutions, and following are their definitions:

- Sybil Attack: An adversary creates multiple fictitious vehicles on the road from a single node/vehicle by allocating it different identities to appear as it represents separate entities. In other words, an attacker creates (and then controls) more than one identity on a single physical node. This implies that other entities in the network will not be able to judge if the data originate from a single vehicle or multiple vehicles. This attack can be used to affect the route selection of a target vehicle by creating a fake traffic jam on the road which forces the targeted victim vehicle to choose an alternative path.
- GPS Deception/Spoofing Attack: It refers to the interception and manipulation of the GPS signals while being sent between two legitimate IoV nodes, to mislead the receiving entity by providing wrong location information about the sending vehicles. This can directly harm the drivers and the passengers by affecting their path decisions. Additionally, when a GPS receiver of a vehicle is attacked, it could provide the vehicle with false information about its location, speed, and other GPS information, which can greatly affect some IoV applications that depend on this GPS information such as navigation devices.
- Masquerading/Impersonation Attack: A node pretends to be another node by stealing its identity. Here, both the legitimate vehicle and the adversary vehicle can use the same identity simultaneously which can create a chaos in the network since other vehicles may receive contradictory information from the same identity. The malicious node can also enjoy the access privileges of the spoofed identity.
- Worm Hole Attack: Also known as tunneling attack, refers to the attack where at least two malicious vehicles create a private tunnel known as a worm hole which is used to forward the intercepted data between the two of them [89]. In this attack, the true distance information is faked where other entities are forced to route through the created tunnel thus controlling all the traffic flowing in the network.
- Replay Attack: In this attack, an adversary keeps iterating the old messages in the network to deceive the other nodes by dropping the messages with high priority from the queue. This can greatly affect the system's efficiency and increase the cost of the bandwidth.

Table 2. Possible security attacks in IoV and VANETs categorized by security requirements.

Attack Targets	Description	Examples	Attack Type
Availability	Attacks that affect the IoV system's availability normally use techniques that can make the bandwidth and transmission power of the IoV system unusable by occupying its maximum resource capacity.	- DoS attack	Active
		- DDoS attack	Active
		- Channel interference attack	Active
Authentication	Attacks that fake the identity of the original sender and act on its behalf, which could be used to spread harmful information in the network.	- Sybil attack	Active
		- Masquerading/Impersonation attack	Active
		- Wormhole/tunnelling attack	Passive/Active
		- GPS spoofing attack	Active
		- Replay attack	Active
Data Integrity	Attacks that tamper with the original message content to badly affect the decisions of the receiving entity which could threaten the overall system.	- Message manipulation attack	Active
		- Malware attack	Active

Table 2. *Cont.*

Attack Targets	Description	Examples	Attack Type
Confidentiality	Attacks that compromise the privacy of data through receiving unauthorized copies of the messages being transmitted between the legitimate sending and receiving entities by an illegal third party.	- Man-in-the-middle attack	Passive/Active
		- Eavesdropping attack	Passive
		- Message holding attack	Active
Routing	Attacks that manipulate the original route of a packet by injecting some malicious recipients in the middle to eavesdrop or even sometimes alter the message before further forwarding it towards its targeted destination.	- Eavesdropping attack	Passive
		- Denial of service attack	Active
		- Masquerading attack	Active
		- Route modification attack	Active

Table 3. Possible attacks on authentication, their targeted OSI layers, and remedies.

Attack	Targeted OSI Layer	Possible Solutions	References
Sybil attack	Network layer	Group signatures, session key certificates, event based reputation system, footprint	[100–103]
GPS deception attack	Physical layer	Dead reckoning, signature-based mechanisms	[104,105]
Masquerading/Impersonation attack	Multi-layer (Physical, Data link, Network, Transport, and Application layers)	Digital certificates, identity-based cryptography	[106,107]
Wormhole attack	Network layer	Geographical leashes	[108,109]
Replay attack	Network layer	Timestamps	[110]

4. Blockchain-Based Authentication Schemes in Vehicular Networks

The focus of this survey as mentioned previously is on blockchain-based authentication mechanisms in vehicular networks. We surveyed a wide range of the existing schemes in the literature and categorized them based on the type of the blockchain used for authentication into three categories: (a) private, (b) public, and (c) consortium blockchain-based authentication. These categories are discussed below.

4.1. Private Blockchain-Based Authentication Protocols

A private blockchain is a limited access blockchain in which only a particular group of trusted entities (which is decided by a network administrator) is granted access permissions to the blockchain transactions for performing specific tasks.

The nature of private blockchains enables establishing a high level of trust during authentication since only a small group of trusted nodes are allowed to access the vehicles' authentication parameters stored in the blockchain. Additionally, being controlled by a single organization allows easier, more efficient management and supervision over the authentication data kept at the ledger. Consequently, private blockchains are implemented by many researchers to serve authentication purpose in IoV platforms.

The authors in [111] incorporated a private blockchain technology with intelligent contract to address the issue of new nodes joining the IoV network. The intelligent contract is designed initially for the verified cloud servers, roadside units and vehicle manufacturers which form a contract node group that use Rayleigh consensus mechanism to authorize or reject the new joining requests. When a new node sends a registration application to join the contract group, each node in the contract node group evaluates the received application and grants its digital signature if it agrees to trust the node, otherwise no digital signature is granted. Then, if 51% of the contract nodes grant their signatures, the node is accepted to the contract node group and a new block is added to the chain. Otherwise, the node's information is added to the list of suspicious nodes and broadcasted to the rest of the

network to block its future joining attempts. This results in suppressing the joining of malicious nodes from the root.

The authors also addressed the authentication of registered vehicles by adopting a Public Key Infrastructure (PKI) technology based on cryptographic accumulator to enhance the authentication efficiency. The authentication process is performed in two phases; the first phase is to verify the vehicle's identity to the roadside unit, and the subsequent phase is the mutual verification between the RSU and the cloud server. In the first phase, the vehicle sends its ID and public key to the RSU which verifies the vehicle identity and adds its own public key to the vehicle information and sends them to the corresponding cloud service provider authority (CA) after encryption with the public key of this CA. Upon receiving the message from the RSU, the CA starts the second phase by first decrypting the message with its own private key, and then searches the vehicle ID and the public key of the RSU in the blockchain to check whether the provided information is correct. If successfully found, a new session key is generated by the CA and sent to the RSU along with the corresponding vehicle ID after encryption with the RSU public key. The RSU decrypts the packet with its private key, stores the session key for securing further communication with the CA, and sends the issued digital certificate to the vehicle encrypted with its public key, upon which the authentication process is culminated.

The proposed solution is evaluated using Veins open-source framework through a small-scale network of 13 nodes in terms of the time overhead and communication cost needed for the encryption process related to the blockchain technology and for the whole authentication process. Their scheme proves to provide high authentication efficiency in preventing malicious attacks with low time and communication costs. However, large packet loss is encountered during the registration of the vehicles and the key distribution process.

The authors in [112] discussed the issue of computing and communication bottlenecks faced by the centralized authentication protocols and single Trusted Authority (TA) schemes that could fail to authenticate the large number of simultaneous vehicle requests within a limited time during high mobility. Thus, they suggested a blockchain-based RSU-assisted authentication and key agreement protocol for a multi-TA network model by offloading part of the authentication process to the RSUs to achieve more decentralization. The aim of offloading is to reduce the resource bottlenecks of the TAs, which results in improving the authentication efficiency. The blockchain technology is used to address the cross-TA authentication issue which is caused by the high mobility of the vehicles in a multi-TA environment. Instead of restarting the whole authentication process when a vehicle exits the coverage area of one TA to the coverage area of another TA, the blockchain adoption allows the new TA to continue the authentication process that was started by the old TA since they manage the same ledger that keeps all vehicle-related information.

The network model consists of four types of nodes: vehicle nodes (VNs) and RSUs which are both considered as untrusted nodes in their threat model, TAs which are assumed to be semi-trusted nodes, and a data center (DC) which is assumed as a fully trusted network entity that stores all vehicle-related information. A smart contract is used to automate part of the authentication process and the delegated proof-of-stack [113] is adopted as a consensus mechanism for more efficient resource utilization and power consumption. The whole scheme is composed of three phases, namely the initialization phase, the registration phase, and the authentication phase. In the initialization phase, the system administrator generates a master key and sends it to all RSUs and TAs. Each VN must be registered with the nearest TA during the registration phase in which a unique ID is granted to it and kept as a record with a unique pointer P in the ledger as well as in the vehicle's memory. The pointer P is then broadcasted to all TAs which jointly pack it into a new block and link it to the previous block in the chain.

The authentication phase has five steps. In the first step, the VN enters the RSU communication range and issues an authentication request to the RSU. Then, the RSU forwards a part of the request message to the TA in the second step asking for the VN-

related authentication parameters. In the third step, the TA executes the smart contract in the blockchain. It checks first whether P exists in the blockchain, then retrieves the VN-related authentication parameters from the DC according to P, and then sends these parameters to the RSU. Once the RSU successfully authenticates the TA and the VN, it sends the updated parameters to the VN and the TA in the fourth step. In the final step, after the TA successfully authenticates the RSU, it sends the updated parameters to the DC via the secure channel. Once the DC has updated the parameters, the TA sends acknowledgment message to the RSU. After the VN successfully authenticates the TA, it updates the authentication parameters in its memory. After the VN and the TA negotiate a session key, it remains valid as long as the VN lies within the communication range of the RSU. Once the VN leaves the communication range of the RSU, the session key will be revoked.

A detailed security analysis is performed on the proposed scheme using ProVerif tool [114] to check its robustness against different security attacks. The results prove that the scheme can resist eavesdropping attack, replay attack, VN impersonation and VN capture attacks, TA and RSU spoofing attacks, and jamming attack. It also guarantees backward/forward secrecy and VN anonymity.

The authors in [115] proposed a protocol termed as "BlockAPP" which serves for both authentication and privacy preservation of vehicles identities. The system architecture contains a registration server and multiple service providers. The registration server is responsible for validating and managing vehicles identities whereas the service providers perform the authentication process. The registration server can only write to the blockchain whereas the service providers have both read and write permissions on the blockchain. Further, two types of blocks are defined within their blockchain, i.e., one is created by the registration server to keep a log of the registered vehicles and the other is added by the service providers to keep track of the access history.

The proposed scheme has three phases: the registration phase where the vehicles interact with the registration server, the authentication phase and the authorization phase which are handled by the different service providers. The registration phase starts when the vehicle sends a registration request message containing its original id (i.e., driver's license or vehicle registration number) to the registration center and then a key exchange process takes place using the Elliptic Curve Diffie Hellman (ECDH) key exchange protocol [116] to exchange their public keys. After which the registration server generates a pseudo id by encrypting the vehicle's original id with its session public key and sends it to the vehicle. Upon receiving an acknowledgement from the vehicle, the registration server adds a transaction with the vehicle-related information to the blockchain after validation. A vehicle then sends a message containing its pseudo id and the session parameters obtained from the previous phase to a service provider which authenticates the vehicle's identity by comparing the received data against the vehicle's information kept in the blockchain. If matched, the vehicle is successfully authenticated, and an access log transaction is added to the blockchain by the service provider. The vehicles can then apply for various services during the authorization phase by sending a service request message with the digital signature of the service. The use of pseudo ids for authentication instead of original ids while restricting their validity to only one session, not only protects the privacy of vehicles but also prevents the system from identity spoofing attacks.

The authors in [117] suggested a secure mutual authentication scheme with reduced dependency on certification authority (CA) by introducing a private blockchain framework. In addition to vehicles, the physical entities involved in their model are the CA and the revocation authority (RA) which both have complete control over the blockchain. The RSUs, on the other hand, have only read permission over the blockchain.

The scheme is composed of three phases, namely, system initialization, registration of the vehicles, and mutual identity authentication and revocation. In the first phase, the CA initializes the system parameters including the elliptic curve parameters and hashing functions. Moreover, the public key pairs are generated and transferred to the blockchain

network entities, i.e., CA, RA, and RSUs. When a vehicle first registers with the CA, it submits its original vehicle id obtained from the motor vehicle's division. The CA verifies the vehicle's original id and assigns for it a Pseudo Id (PID) along with the Elliptic Curve Cryptography (ECC) public–private key pair. The PID is then signed digitally by the CA using the Elliptic Curve Digital Signature Algorithm (ECDSA) [118], forming a new transaction which is added to the blockchain under the proof-of-authority consensus mechanism among the multiple CAs. When the vehicle's registration information, i.e., PID and the digital certificate, is added successfully to the blockchain, a pointer referring to its storage location in the blockchain along with a unique transaction id are sent back to the CA. At this point, the CA transfers the pointer, the PID, the certificate along with the ECC key pair to the vehicle's OBU. The CA also stores a record mapping the real identity of the vehicle to the Pseudo identity in the hash table in its local database which helps facilitate the lookup in the case of traceability and revocation of malicious vehicles.

When the vehicle becomes active on the road, it initiates an authentication request containing its PID, hash pointer, and transaction id to the nearest RSU. The RSU then uses the received PID as an index to query the blockchain for the vehicle's respective transaction, if verified, the RSU sends a challenge message to the vehicle encrypted with its public key and waits for the reply. If the vehicle successfully decrypts the challenge message and sends the correct response, it is authenticated successfully by the RSU. Extensive simulation using Vein's framework and OMNeT++ network simulator proves the efficiency of this scheme in terms of authentication delay, transaction throughput, and packet-delivery ratio.

The authors in [119] proposed a distributed message authentication scheme using a private blockchain, where vehicles can authenticate the messages broadcasted in the network in a distributed manner. The system model is composed of a single Root Trusted Authority (RTA), multiple Local Trusted Authorities (LTAs), RSUs, and vehicles. The RTA is a fully trusted authority that is responsible for managing the entire system and performing the registration process whereas the individual LTAs are responsible for authenticating the vehicles in their local areas. The authors define two types of nodes based on the task they perform on the blockchain, namely, block generation nodes and block verification nodes. The generation of blocks is performed through the proof-of-work consensus mechanism and is assigned to the infrastructure nodes, i.e., LTAs due to their high computing capability, while the verification of the blocks is the responsibility of the vehicles. Since the vehicles are highly mobile and have a relatively low computing power, the consensus during block verification must be completed quickly, and thus the use of the Practical Byzantine Fault Tolerance (PBFT) consensus mechanism.

The proposed message authentication scheme includes six phases: initiation, registration, message signing, message verification, block generation, and block confirmation. In the initiation phase, the RTA generates its public–private key pair, the genesis block of the blockchain and the list of LTAs. During the registration phase, a vehicle's owner sends the vehicle's information and its biometric information to the RTA which in turn generates a pair of asymmetric keys and transfers it along with the system key to the vehicle's local memory. The registration of LTAs also takes place in this phase by the RTA in the same approach as the vehicles' registration. When a vehicle needs to broadcast a message into the network, it computes the message's hash value h(m) and concatenates it with the hash values of the previous blocks in the blockchain and encrypts them together with its private key. This arrangement is then attached as a header to the actual message content along with a timestamp and encrypted with the system key before being broadcasted to other vehicles. This process of message signing guarantees the legitimacy of the sending vehicle and thus the authenticity of the broadcasted information since the unauthorized vehicles cannot have the system key used for message signing as it is distributed only to the registered vehicles during the registration phase.

As the V2V messages are broadcasted among the vehicles, the corresponding LTA keeps collecting those messages until it forms a block after a certain number of messages. The block is then verified through the PBFT consensus by the vehicles and their LTA. Once

the block is verified, the LTA transfers it to the other LTAs for block confirmation process. If confirmed by all LTAs, they send the confirmed block to the RTA which then concatenates the block officially into the blockchain. The simulation results reveal that the proposed scheme can prevent impersonation attacks and single point of failure issue while providing a highly efficient blockchain-based authentication in terms of the total consensus delay and throughput.

The above-mentioned private blockchain-based authentication schemes can be found in Table 4 for easy reference.

Table 4. A comparative study of the private blockchain-based authentication schemes in IoV and VANETs.

Ref.	Technique	Attack Counteracted	Network Model and Entities (Other than Blockchain)	Evaluation	Metrics	Features and Limitations	Privacy Preservation of Vehicle's Identity?
[111]	- Rayleigh consensus mechanism - Intelligent contract - PKI based on password accumulator	- Not specified	- V2I - vehicles - RSUs - Trusted centre (cloud service provider)	- Veins simulation tool (OMNeT++ and SUMO)	- Computational cost (16.5 ms) - Communication cost (50 KB)	- Provides an efficient key distribution mechanism based on crypto-accumulator - Provides mutual authentication and key exchange - Large packet loss in the vehicle registration and key distribution process - No security analysis	No
[112]	- -Delegated Proof-of-Stack (DPoS) consensus mechanism - Smart contract	- Eavesdropping - Replay - VN capture and VN impersonation - RSU and TA spoofing - Jamming - Session fixation - Wrong password login/update	- V2I - Vehicle nodes - RSUs - Trusted authorities - Data centre	- ProVerif tool	- Computational cost (0.434 ms) - Communication cost (4416 bits)	- Supports an efficient cross-TA authentication - Improves the authentication efficiency through offloading part of the computational load to the RSUs to reduce the TAs' resource bottleneck - Lightweight in computation - Does not consider the design of the communication protocol between the TAs and the DC and relies on assuming a secure channel between them, which is so idealized and lacks rationality	Yes
[115]	- Smart contract - Asymmetric key cryptography	- Identity spoofing	- V2I - Vehicles - RSUs - A single registration server - Multiple service providers	- Software implementation using Solidity language on Remix platform	- Not specified	- Supports an optional traceability feature. - Supports conflict-free access-log maintenance. - No performance evaluation	Yes

Table 4. *Cont.*

Ref.	Technique	Attack Counteracted	Network Model and Entities (Other than Blockchain)	Evaluation	Metrics	Features and Limitations	Privacy Preservation of Vehicle's Identity?
[117]	- Proof-of-Authority consensus mechanism - Elliptic curve discrete logarithm problem - Elliptic Curve Digital - Signature Algorithm	- Impersonation	- V2I - OBUs - RSUs - Certificate authority - Revocation authority	- OMNeT++ (Objective Modular Network Testbed in C++) - Veins simulation tool	- Communication delay (45 ms for up to 5 vehicles) - -Throughput (45 bits/s for up to 5 vehicles) - Packet delivery ratio (90% up to 35 vehicles, then drops with increasing traffic from 35 to 50 vehicles)	- Provides mutual authentication with reduced dependency on the CA thus reducing the overall communication overhead - Ensures data confidentiality, integrity, and non-repudiation - Supports fast revocation of vehicles without extra overhead - No single point of failure - Does not fully explore the characteristics of the blockchain technology such as the use of smart contracts	Yes
[119]	- Proof of Work (PoW) consensus mechanism - Practical Byzantine fault tolerance (PBFT) consensus mechanism - Elliptic curve cryptography (ECC) - AES-256	- Internal impersonation	- V2I - Vehicles - RSUs - A root trusted authority - Local trusted authorities	- Simulation model implemented with Python	- Total consensus delay (increases linearly from 2 s at 25 vehicles to 10 s at 150 vehicles) - Transactions per second (decreases exponentially from 50 TPS at 25 vehicles to 10 TPS at 150 vehicles)	- Guarantees message integrity - Ensures non-repudiation and traceability - Prevents single point of failure - Large delay in consensus making	Yes

4.2. Public Blockchain-Based Authentication Protocols

A public blockchain is an open access blockchain in which everyone can access, send, receive, and verify the different transactions of the blocks. Since it is a fully opened blockchain, even the vehicles can participate in the authentication process by looking up the ledger for the targeted authentication parameters. This provides a better utilization of the available computing resources in the IoV environment compared to restricting the authentication process to a few trusted nodes, thus a more decentralized, time efficient authentication process is achieved. These characteristics of a public blockchain have attracted many researchers to adopt it for IoV authentication.

The authors in [120] contributed to address the authentication delay issues and time complexity in IoV network. The proposed work provides real-time authentication and adversary detection through the adoption of a public blockchain. The authors used the wireless channel characteristics, such as the received power and the Link Fingerprint (LF) along with the hash technology of blockchain to detect any intrusion in V2V communication in real-time. The main concept is that the wireless link between any two communicating vehicles has a unique fingerprint which is generated from the channel's power characteristics. As a result, the variation in the received power of the communicating vehicles must highly correlate, otherwise the communication path is intercepted, and an adversary is detected. Each vehicle uses the LF, a pseudo-random freshness parameter N, (that changes every time to prevent the system from replay attacks), and the hash of the previous block used to generate the hash value. The hash is then stored in its local memory and sent to the cloud to be stored in the publicly accessible ledger. A sending vehicle encapsulates the

packet with a header containing its hash value before being sent to the receiving vehicle. When the receiving vehicle gets the packet, it removes the packet header and looks up the hash value in the ledger to check the authenticity of the sender vehicle, if it exists, it accepts the package data; otherwise, an adversary is detected, and the packet is discarded.

MICAz mote—a hardware wireless sensor module—is installed on two vehicles to serve as a wireless communication interface in the V2V arrangement. Measurements are recorded indoor and outdoor in real-time and reported with the aid of MATLAB R2020a. The Pearson Correlation Coefficient [121] is computed to detect an adversary in the network when its value is less than or equal to 0.9. The scheme is also evaluated in terms of time complexity which is found to be as low as O(1) due to the simple and lightweight hash function used in their blockchain.

The authors in [122] proposed a scalable blockchain-based protocol that deploys a dynamic proof-of-work consensus mechanism and Physical Unclonable Functions (PUFs) for authentication and trust establishment. Their approach depends on the assumption that the smart vehicles are equipped with PUF components that generate hardware fingerprints which serve as unique identities replacing passwords and secret keys. The authentication process passes through two phases, namely the setup phase and data transfer phase. The vehicle's registration process is performed during the setup phase, where each vehicle is given a pair of public and private keys and allocated an account address in the blockchain. A smart contract named "enforcer" is utilized to initiate the communication between the vehicles and the blockchain whereas the RSUs serve as the blockchain miners and the certificate authority as well. When a vehicle generates data traffic, the enforcer first checks its existence in the list of registered vehicles stored in the RSUs. If it is registered, a PUF challenge is then sent to the vehicle. If the vehicle succeeds in this challenge, the authentication is completed successfully, and a communication link is established between the vehicle and the local blockchain. A digital certificate is then issued by the RSU to the vehicle to serve anonymity and privacy preserving purposes for future authentication process.

After registration and successful authentication, a vehicle can communicate with other entities in IoV environment and exchange data in the data transfer phase. The deployed dPoW consensus mechanism allows the protocol to scale based on the incoming traffic generated by the vehicles and their use of PUFs makes the vehicles immune to physical and impersonation attacks. A detailed analysis is conducted through software implementation and NS3 simulation tool to evaluate their scheme in terms of the four-way tradeoffs of distributed systems which are scalability, decentralization, security, and latency. Two types of delay were measured: (1) the authentication delay at the RSU, which is time needed to authenticate a vehicle by the RSU and (2) the time to finality, which is the time needed to form a block, mine it, and reach a consensus on the mined block. The results show that their authentication scheme efficiently satisfies all the above-mentioned four properties without sacrificing any of them.

The authors in [123] designed a novel blockchain-assisted authentication scheme for Artificial Intelligence (AI)-envisioned IoV-enabled smart cities called "BBAS-IoV" by which authentication is performed both individually and in batches. The network model is composed of several smart cities; each is managed by a separate Trusted Authority (TA) and divided into multiple clusters. Each TA is responsible for initializing the system parameters during the initial setup phase, registering RSUs and vehicles within its service area during the registration phase and distributing certificates and private/public key pairs later to them. The model contains a fog server connected to each group of geographically related RSUs and a group of cloud servers forming the publicly accessible blockchain center.

Beside the setup and registration phases, the protocol has other six phases, namely, message signing, authentication, group key management, blockchain formation, AI-based secure big data analytics using blockchain and dynamic nodes addition. During the authentication phase two types of authentications exist, i.e., V2V and batch authentication. The V2V authentication enables each vehicle to authenticate its neighbors in its cluster in the smart city. The batch authentication is then used by the RSU to authenticate all its

clusters' vehicles simultaneously which saves time and reduces the computation overhead of the whole scheme. After that, a group key is agreed upon and granted to each cluster to be used for securing communication among intra- and inter-cluster vehicles and their managing RSU. The blockchain formation phase is handled by fog and cloud servers in two steps; first, each fog server receives the list of transactions and their compact signatures from the associated RSUs and verifies them, if the signatures are valid, it transmits the partial blocks to a cloud server in the blockchain center. Then, the cloud servers convert the received partial blocks into complete blocks which are then mined and voted for through the PBFT consensus mechanism to decide on their eligibility to be added to the blockchain. The signature verification and block verification applied in this scheme ensures that data poisoning attacks which inject malicious transactions in the blockchain are avoided in the proposed BBAS-IoV protocol. This results in fully trusted blockchain transactions that can be a great asset for deriving highly accurate ML models and thus correct predictions and decision making can be achieved.

Detailed formal security analysis using the Automated Validation of Internet Security Protocols and Applications (AVISPA) tool as well as informal security analysis is provided to evaluate the security features of the proposed BBAS-IoV scheme. The results obtained show that various security attacks namely, replay attacks, man-in-the-middle attack, vehicle and RSU impersonation attacks, privileged-insider attack, and ephemeral secret leakage attack are prevented. Extensive performance evaluation through simulation with the aid of Multi-precision Integer and Rational Arithmetic Cryptographic Library (MIRACL) reflects high efficiency of the scheme in terms of computation, communication, and storage overheads.

The authors in [124] designed a blockchain-based authentication scheme for vehicular accident detection and notification in IoV-enabled intelligent transportation systems, called BCAS-VADN. The scheme deploys a cloud/edge computing framework that consists of cloud servers, edge servers, RSUs, and vehicles. The system architecture is divided into multiple clusters with a Cluster Head (CH) for each, which acts as an intermediate entity to arrange the communication between the cluster members and the RSUs. Each RSU is associated with an edge server and all edge servers are linked to cloud servers in the blockchain center through a public channel. The proposed scheme consists of five phases, namely, system initialization, enrollment, authentication, blockchain verification and addition, and dynamic node addition phases.

The proposed scheme assumes the existence of a trusted registration authority that is completely responsible for initializing the system parameters including elliptic curve, one-way hash function and its own private–public key pair as well as enrolling all the entities in the network, i.e., cloud servers, edge servers, RSUs, and vehicles. The authentication phase then takes place in two steps: V2CH authentication in which a vehicle and its associated CH mutually authenticate, then CH2RSU authentication where the CH and its associated RSU authenticate each other. Upon a successful authentication process, each vehicle can securely report accident-related transactions to its associated CH if it detects an accident on the road. The cluster head then securely transfers the received transactions to its associated RSU which in turn sends them secretly to the corresponding edge server. The edge server prepares a partial block containing the accident-related transactions, the Merkle tree root, and a digital signature. This incomplete block is forwarded to its associated cloud server in the blockchain center forming a complete block from the received partial block. At this point, all the cloud servers in the blockchain center participate in the block verification process through the PBFT consensus and if verified, the complete block containing the vehicle accident-related information is added to the blockchain center and made available for use by other vehicles for optimal route selection and better road-related decisions.

Using the Automated Validation of Internet Security Protocols and Applications (AVISPA) simulation tool, the proposed BCAS-VADN proves to be secure against multiple attacks including replay, man-in-the-middle attacks, impersonation and privileged-insider attacks, physical vehicle capture attack, and ephemeral secret leakage attack.

The authors in [125] introduced a scheme for securely authenticating the vehicles and the messages exchanged in the network using a public blockchain, called BCPPA. The scheme employs the Elliptic Curve Digital Signature Algorithm (ECDSA) but supports replacing it by an improved signature scheme to enable batch authentication. The BCPPA protocol consists of three phases: system initialization, message signing, and message verification. For improved security, the system initialization is performed by both the vehicles and the certificate authorities via the private-type derivation and the public-type derivation processes. The private-type derivation is performed by the vehicles to generate a root private key which is kept at the vehicle's OBU to be used later to derive a fresh private key for each future communication. A corresponding public key is also generated by the vehicle and sent to the certificate authority which uses it to generate the new public key and certificate in the public-type derivation process. The public blockchain is used in this scheme to store the public certificates which are embedded into the transactions so that the vehicles can obtain the certificates from the blockchain instead of preloading all of them in the OBUs, which helps mitigate the storage burden of the vehicles. In the message signing phase, a vehicle that needs to broadcast a message to other vehicles in the network must sign the message by first executing the private-type derivation to obtain the current private key and then triggering the smart contract to obtain the transaction id that keeps the public certificate corresponding to the generated private key. The receiver then verifies whether the received message/signature pair is valid or not, if valid, the received traffic is accepted, and decisions can be made based on it.

Extensive simulation using Vanet-MobiSim and NS2 demonstrates that the proposed BCPPA can resist several attacks such as replay attack, impersonation attack, DDoS attack, man-in-the-middle attack, stolen verifier attack, side-channel attack, message modification attack, birthday collision attack, and hijacking attack. The authors claim good efficiency in terms of communication cost, time cost, average packet delay, and packet loss ratio.

The authors in [126] proposed a lightweight Decentralized Key Management Mechanism with Blockchain (DB-KMM) and bivariate polynomial. The network model involves three types of entities: Vehicle Service Provider (VSP), Blockchain Network (BN), and the vehicles. The VSP is responsible for deploying the BN and the smart contract, issuing the transaction data, registering, updating, and invalidating the vehicles' public keys. The BN is constructed by the RSUs which are responsible for creating and mining the new blocks through the PoW consensus mechanism while providing public keys and services to the vehicles. The proposed DB-KMM is composed of six phases, namely, system setup, registration, authentication, key agreement, public key update, and public key revocation. In the system setup phase, the VSP derives the system parameters such as the ECDSA and the Elliptic Curve Integrated Encryption Scheme (ECIES) parameters, the bivariate function parameters as well as initializing the smart contract. Each vehicle that aims to join the VANETS network must register itself through the VSP which generates for it a pair of public and private keys while registering the public key in the smart contract. When a vehicle needs to communicate with other VANETS entities, it first mutually authenticates with the nearest RSU. Once the mutual authentication succeeds, a key exchange mechanism takes place between the vehicle and its corresponding RSU in order to agree on a shared session key for securing the subsequent communication.

The DB-KMM provides an automatic public key management including update and revocation via the smart contract. For the update process, when a vehicle sends a key update request containing its ID, old public key, and validity period to the VSP, the VSP triggers the smart contract to generate a new public/private key and a new validity period for the requesting vehicle. The VSP then forms a new transaction containing the vehicle ID, new public key, and validity period and sends it to the BN. The RSUs forming the

blockchain network perform the consensus on the received transaction and if the mining succeeds, the updated transaction is added to the blockchain, and the new public key is transferred to the requesting vehicle. Lastly, when a malicious behavior is noticed on some vehicle, the VSP initiates a revocation transaction to the BN and triggers the smart contract to remove the vehicle's identity and public key from the blockchain.

The performance of the proposed DB-KMM is tested in terms of the end-to-end packet latency and the packet loss ratio using OMNeT++ and Veins simulators and the results prove that it greatly improves the cost of public key management compared to the traditional PKI management. Further, security analysis shows that the scheme can resist DoS attack, public key tampering attack, internal attacks, as well as collusion attacks.

The authors in [127] extended the conventional blockchain by introducing two novel data structures called the Merkle Patricia Tree (MPT) and the Chronological Merkle Tree (CMT) and then proposed a Blockchain-based Privacy Preserving Authentication scheme (BPPA) based on this extended blockchain. The system model includes the following entities: certificate, certificate authority, Law Enforcement Authority (LEA), RSUs, and vehicles. The certificate includes the public key, the expiry date, the timestamp, and the encrypted mapping between the vehicle's real identity and its certificates. The certificate authority issues two types of transactions: the issuance transaction which includes the issued certificate, the timestamp and the signatures of the trusted authorities, and the revocation transaction which contains the revoked certificate. The LEA is responsible for the registration of vehicles and monitoring their behavior. Additionally, it concatenates and organizes the transactions received from the certificate authority to generate a block and transfers the block to all the RSUs for verification. When a certificate issuance transaction or a certificate revocation transaction is broadcasted by the certificate authority, a leaf node is inserted into or removed from the MPT, respectively, and the root of the MPT is updated. The transaction and the corresponding root of MPT are recorded chronologically in the CMT.

The root of CMT is considered as the transaction root whereas the root of MPT is taken as the certificate root. The transaction root and the certificate root are then written immutably in the blockchain. The significance of this extended blockchain being developed is represented by two aspects. First, it provides a simplified authentication technique whether a certain certificate is in the MPT or not. Given the certificate root and a record containing the nodes along the path, the authenticator can compute a hash using the given record. If the hash value is equal to the certificate root in the blockchain, it is proven that the certificate exists in the MPT. Second, it provides transparency within the activities of the authorities by using transactions roots; since, if the transaction root is given, it can be verified when a certain certificate is issued or revoked. Conditional privacy preserving is provided by allowing each vehicle to utilize several certificates, while the mapping between the certificates and the real identities is encrypted by the LEA's secret key and stored in the blockchain and can only be revealed by the LEA in case of malicious behavior. Security investigation proves that BPPA is resistant to forgery attack, man-in-the-middle attack, replay attack, identity revealing attack, and authority abuse attack. Further, experimental results demonstrate the efficiency of the scheme in terms of communication and computation costs, low latency, and high throughput.

The above-mentioned public blockchain-based authentication schemes can be found in Table 5 for easy reference.

Table 5. A comparative study of the public blockchain-based authentication schemes in IoV and VANETs.

Ref.	Technique	Attack Counteracted	Network Model and Entities (Other than Blockchain)	Evaluation	Metrics	Features and Limitations	Privacy Preservation of Vehicle's Identity?
[120]	Link fingerprinting	Replay	- V2V - 2 vehicles - (With MICAz mote mounted on each) - Fusion centre (Cloud server)	- Hardware implementation using MICAz motes - Simulation using MATLAB R2020a	- Pearson Correlation Coefficient - Computational time (s)	- Provides real-time adversary detection. - Lightweight in computation - Lack of security evaluation	No
[122]	- Dynamic Proof-of-Work (dPoW) consensus mechanism - Smart contract - PKI - Physical unclonable functions	- Cloning - Impersonation - Data tampering	- V2I - Vehicles - RSUs - Miners - Cloud storage - PUFs	- Software implementation (using Solidity for smart contract and Python for dPoW) - Simulation using SUMO and NS3	- Communication overhead (bytes) - Latency (s) expressed in 2 measures: - 1—Authentication delay at RSU - 2—Time-to-Finality - MAC and physical layers bytes overhead (%)	- Supports scalability according to the incoming traffic - Satisfies all the four-way trade-off properties (scalability, decentralization, low latency, and security guarantee) - Provides physical protection through the PUFs	Yes
[123]	- PBFT consensus mechanism - Symmetric key: Advanced encryption standard - Asymmetric key: Elliptic curve discrete logarithm problem - Bilinear pairing	- Replay - Stolen verifier - Data poisoning - Man-in-the-middle - Privileged-insider - Vehicle and RSU impersonation - Ephemeral secret leakage	- V2I - Vehicles - RSUs - Trusted authorities - Fog servers - Cloud servers	- Automated Validation of Internet Security Protocols and Applications, simulation tool for formal security analysis - MIRACL: library for measuring the execution time of the different used cryptographic techniques	- Storage overhead (2720 bits) - Communication cost - (Single and batch verification) - group key management - Computation cost - (V2V single authentication and V2RSU batch authentication)	- The genuineness and authenticity of blockchain data supports the use of big data analytics to machine learning and AI applications - Supports batch authentication which saves time and reduces the computational overhead - Does not provide practical implementation on the claimed support for big data analytics, AI, and ML	Yes
[124]	- PBFT consensus mechanism - Elliptic curve discrete logarithm problem (ECDLP) - One-way hash function - ECDSA	- Replay - Man-in-the-middle - Impersonation - Privileged-Insider - Physical vehicles capture - Ephemeral secret leakage	- V2I - Vehicles - RSUs - Registration authority - Edge servers - Cloud servers	- Automated Validation of Internet Security Protocols and Applications (AVISPA) simulation tool for formal security verification	- Communication cost (2400 bits) - -Computation cost (227.6 ms)	- Enables vehicle accident detection and notification - Supports mutual authentication and key agreement - Does not discuss the blockchain-related evaluation measures, i.e., the throughput (TPS) and the blockchain's storage overhead	Yes

Table 5. *Cont.*

Ref.	Technique	Attack Counteracted	Network Model and Entities (Other than Blockchain)	Evaluation	Metrics	Features and Limitations	Privacy Preservation of Vehicle's Identity?
[125]	- PoW consensus mechanism - Smart contract - ECDSA	- Hijacking - Impersonation - Message modification - DDoS - Replay - Man-in-the-Middle - Stolen verifier table - Side-channel	- V2V - Vehicles - RSUs - Certificate authorities	- Vanet-MobiSim simulation tool - NS2 simulation tool	- Time cost (0.017974 s). - Communication cost (264 byte) - Average packet delay (APD in s) - Packet loss ratio (PLR in %)	- Supports batch verification - Does not consider the real-world factors in security and performance evaluation	Yes
[126]	- PoW consensus mechanism - Smart contract - Bivariate polynomial - ECDSA - ECIES	- Internal - Public key tampering - DoS - Collusion	- V2I - Vehicles - Blockchain network: consists of the RSUs - Vehicle service provider	- OMNeT++ event simulator - Veins network simulator - OMNeT++	- Computation overhead (ms) - Communication overhead (657 bytes) - Storage overhead (114.4 MB) - Average end-to-end packet latency (ms) - Average packet loss ratio	- Supports mutual authentication - The authentication process is lightweight - Does not support anonymity during authentication	No
[127]	- Elliptic curve cryptography - ECDSA - Secure hashing algorithm - Advanced encryption standard	- Forgery - Man-in-the-middle - Replay - Identity revealing - Authority abuse	- V2I - Vehicles - RSUs - Certificate authority - Semi-TAs - Law enforcement authority	- Testbed (2 laptops as RSUs and 6 laptops as vehicles connected through 1 Gb/s switch) + Software implementation using Python	- Transaction throughput (transactions/s) - Transaction latency (ms) - Time consumption (ms) - Communication overhead (KB)	- Supports a conditional privacy - Ensures integrity and non-repudiation - The scheme is evaluated on a small-scale IoV platform (only 2 RSUs and 6 vehicles) which is not enough to prove its efficiency in real-world scenarios	Yes

4.3. Consortium Blockchain-Based Authentication Protocols

A consortium blockchain, also known as hybrid blockchain, is a combination of both private and public blockchain in which the read access can be open or restricted, and only a small group of nodes belonging to different organizations is responsible for making the consensus.

Since consortium blockchains incorporate the best of public and private blockchains, that is, a mixture of decentralization with good level of trust at the same time, it has been the most popular blockchain type being implemented by researchers for IoV authentication. In such way, the authentication can be performed with a high degree of trust since only a group of trusted entities perform the consensus of the authentication data blocks, while guaranteeing an efficient performance in terms of resource utilization and authentication time delay due to the semi-decentralized nature of consortium blockchains.

The authors in [128] optimized the Byzantine consensus algorithm by adopting time sequence and gossip protocol [129] to validate IoV information for correctness before adding them to the consortium blockchain. The use of gossip protocol, specifically the push–pull mode, enables faster data exchange among IoV nodes, as each two neighboring nodes can have the same information in one cycle. Two types of nodes are defined in the proposed scheme, i.e., Vehicle Communication Nodes (VCNs) and Roadside Communication Nodes (RCNs) in addition to the blockchain cloud platform used as storage for all IoV data. Due to their high computing and storage capabilities, RCNs are used as consensus-makers in the proposed Byzantine Consensus Algorithm with Time-sequence and Gossip protocol

(BCA-TG). To ensure data integrity and authenticate the data sources, any data generated by a VCN or RCN must be agreed upon by more than half of the RCNs for the new block to be granted and linked to the blockchain.

In the BCA-TG protocol, each RCN has an Update Information (UI) vector containing the Local Information (LI) of all RCNs in the consensus network as elements. Initially, the UI of each RCN will have only its own LI while all the other LI elements corresponding to the other RCNs are set to null. For example, if 5 RCNs are used for consensus making, the UI of RCN^1 is initially: $UI^1 = \{LI^1,0,0,0,0\}$. After which each RCN starts to communicate its UI vector with the neighbors in its view through the push–pull mode of gossip protocol until all RCNs have UIs with no null values. At this point, the element which forms more than half of the elements in the updated UI vector is considered the true information or the Consensus Information (CI) that will then be added to a new block and linked to the blockchain. The proposed scheme proves to have high fault tolerance since it can determine the CI even if the faulty or Byzantine nodes form 49% of the network. Moreover, their use of time sequence provides high scalability through its control over the entry and exit of nodes to/from the network and better convergence speed is achieved compared to the ordinary Byzantine consensus algorithm.

The authors in [130] handled the cross-datacenter authentication issue in Vehicular Fog Computing (VFC) environment by proposing BLA—a Blockchain-based Lightweight Anonymous authentication scheme. The system model consists of multiple regions; each region is managed by a Service Manager (SM) which is responsible for authenticating all OBUs and managing all Vehicular Fog Datacenters (VFDs) represented by the RSUs in its region. A Witness Peer (WP) exists in each region to write the authentication logs to the ledger maintained by the corresponding SM. The ledger is only accessible by the members of the consortium blockchain, such as the SMs, the WPs and the audit department which is assumed to be a fully trusted authority responsible for registering all the network entities underneath.

The RSUs within a region serve as access points to the vehicles in the IoV paradigm and also as fog computing units for providing real-time services to authorized OBUs. The proposed BLA protocol includes five phases: initialization, registration, authentication, consensus, and service-delivery phases. The initialization phase takes place only once via the initial setup of system parameters by the audit department. Then, the registration of SMs and OBUs is conducted by the audit department during the registration phase in which each registered entity is allocated a pair of private and public keys using Elliptic Curve Cryptography (ECC) and Diffie–Hellman (DH) cryptography mechanisms. During the authentication phase, each SM authenticates the OBUs within its region, and the authentication results are then passed to the subsequent phase where they are written to the ledger by the consensus makers, i.e., WPs, through PBFT consensus protocol. The way they addressed the cross-datacenter authentication is by allowing a flexible option to vehicles to choose whether to be reauthenticated or not upon entering a new VFD during the service-delivery phase.

The noninteractivity property that BLA has, in which a vehicle sends only one message to its SM for authentication or service requesting without the need for exchanging any acknowledgement messages between them, makes it lightweight in both communication and computation cost. In addition, the utilization of pseudonym preserves the privacy of vehicles and ensures anonymity. Security analysis proves that the proposed BLA protocol ensures most of the security aspects in IoV network, such as confidentiality, integrity, traceability, and non-repudiation. Moreover, extensive simulations are performed to measure the performance in terms of response time. The results obtained show that low time overhead is achieved which reflects the suitability of BLA algorithm for real-time VFS.

The authors in [131] improved the reliability of the authentication scheme proposed in [130] through the adoption of mutual authentication and key exchange mechanism. During the authentication phase, instead of just allowing one-way authentication in which only the SMs can check the authenticity of vehicles [130], a two-way authentication is

enabled in [131] where a SM first authenticates the identity of a vehicle using the ECC then the vehicle authenticates the communicating SM in the same way. Upon successful mutual authentication, a session key is established and exchanged between the two parties for securing their future communication; which is a prerequisite for secure authentication protocol, unlike the work done in [130]. Moreover, the scheme guarantees the forward secrecy. The timestamps used for generating the authentication parameters prevent replay attacks. An extensive performance evaluation and comparison is conducted which reveals that the proposed solution outperforms the work in [130] in terms of communication and computational overheads.

The authors in [132] proposed a Blockchain-based Privacy preserving Authentication System (BPAS) for VANETs which supports password and biometric login-based authentication. BPAS relieves the overhead of having an online registration center during the authentication phase by providing a TA-independent authentication scheme in which vehicle's authentication is handled by RSUs or other vehicles in the network. However, the TA is responsible for other system phases namely, system initialization, smart contract deployment, vehicle registration, and vehicle revocation phases. The scheme deploys a technique based on fuzzy extractor for biometrics extraction and an Attribute-Based Encryption (ABE) scheme to protect the privacy of users by encrypting their blinding identities to ensure that no other entity can decrypt them except for the blockchain managers.

During the system initialization phase, the TA initiates the system parameters including the ECC, the ABE, and the blockchain parameters. A smart contract is then deployed by the TA into the blockchain to automate the authentication process. Each vehicle then needs to be registered with the TA to obtain its secret authentication parameters during the registration phase. First, the owner of a vehicle must choose a physical identity, a password along with his/her biometrics which will be sent to the TA. The TA then calculates a corresponding blinding identity (AID) and a Vehicle Public Key (VPK) from the received parameters and uploads them as a unique tuple {AID, VPK} to the Vehicle Public Key Table (VPKT) in the smart contract. The AID is also sent to the vehicle's OBU which is assumed to be tamper-proof. When a vehicle wishes to send data to nearby vehicles or RSUs, the vehicle's owner provides the login information (i.e., password and biometrics) which are verified by the OBU. If correct, the OBU encrypts the vehicle's AID using the ABE and sends it along with the message and a timestamp to the receiver (i.e., a vehicle or RSU), otherwise, the OBU rejects the message. The receiving entity then validates the freshness of the message through the timestamp. If valid, it initiates a transaction to the blockchain managers requesting for the associated vehicle public key. The blockchain managers then lookup the VPKT using the AID to obtain the corresponding VPK which is then transmitted to the transaction issuer to be verified. Upon successful validation, the authentication is completed, and the message is accepted.

BPAS also supports conditional traceability and vehicle's revocation in case of detecting any malicious behavior by simply allowing the TA to delete the corresponding tuple in the VPKT. The proposed scheme is evaluated in terms of time cost and security features and is found to be resistant to replay attacks, impersonation attacks, DDoS, and password guessing attacks.

The authors in [133] proposed an Efficient Authentication Scheme over Blockchain for Fog computing-enabled IoV (EASBF). The authors consider three types of communication in their fog-enabled model, i.e., V2V, V2I, and V2R. Each fog area can provide different services to users and vehicles within its coverage range, and it includes one or more RSUs, one or more CAs, a single Blockchain Manager (BM), and a single Authentication Manager (AM). The CAs are trusted entities responsible for updating and managing the certificates issued for vehicles in their fog areas. The BMs are deployed to manage the blockchain and authenticate the OBUs whereas the AMs write the results of authentication into the blockchain (which together form the consortium blockchain). The PBFT is used for consensus.

The proposed scheme contains five phases: initialization, registration, mutual authentication and key exchange, consensus, and certificate update. A central secured entity, named TA, is responsible for initializing the system and the public parameters used for the cryptographic functions, as well as registering the OBUs and RSUs during the first two phases of EASBF. Then, mutual authentication and key exchange takes place between OBUs and BMs, and a session key is shared among them for subsequent interactions. Upon successful authentication and key exchange, the BM shares the results of authentication with all AMs, which store them into a new block and add it to the large public register under the PBFT consensus. During the consensus phase, one of the AMs acts as a "Speaker" which is responsible for initiating the consensus process while the rest serve as the congress members who participate in the voting scenario initiated by the Speaker. Finally, the certificate update phase which supports two scenarios: the ability to move from one fog area to another transparently without the need of re-authentication and certificate update upon a vehicle's request. The Random Oracle Model (ROM) [134] and AVISPA tool [135] are deployed for formal security verification which proves the resistance of the proposed scheme against DDoS, replay, man-in-the-middle, identity theft, traffic analysis, masquerading, and session key disclosure attacks. Additionally, an extensive performance evaluation shows its efficiency in terms of computation, communication, and storage overheads.

The authors in [136] proposed an approach to address both anonymous authentication and efficient revocation of vehicles in VANETs through the use of pseudo-ids, blockchain, and revocation tags. The scheme defines three types of nodes, namely, a supervisory node which is the Traffic Department (TD), accounting and revocation nodes represented by the multiple TAs, and verification nodes which are the road-side units. The proposed scheme is composed of four phases: initialization, registration, mutual authentication, and expeditious revocation. The privacy of vehicles during authentication is preserved by using the pseudo-ids granted to them by the RSUs. When an RSU generates a pseudo-id for a vehicle during the registration phase, the RSU stores it into a Trusted Cloud Server (TCS) and transfers a pointer referring to the storage location of the pseudo-id to the corresponding TA. The TA then forms a transaction with the vehicle's registration information including its public key certificate, the pointer to its pseudo-id stored in the TCS, and a unique Transaction id (TID) and uploads it to the blockchain. Using this TID, the identity of a vehicle can be later authenticated by viewing the corresponding records in the blockchain.

This arrangement in which the blockchain keeps only pointers to the pseudo-ids while the pseudo-ids themselves are kept in the unlimitedly huge TCS improves the scalability of the system. In addition, an illegal vehicle can be determined by checking whether its pseudo-id has a revocation tab instead of looking up the whole certificate revocation list which greatly reduces the computational overhead. Further, detailed security analysis proves that the proposed scheme can resist replay attacks and prevent single point of failure problem.

The authors in [137] addressed the interference issue caused by the continuous key updating in large-scale VANETS environments by proposing a blockchain-based framework for secure authentication and efficient group key updating in edge computing-enabled VANETs. They proposed a mutual V2R authentication scheme that employs certificateless cryptographic mechanisms in order to avoid the key escrow issue. The system model consists of a cloud layer which serves as a trusted authority, an edge layer represented by the distributed RSU clusters, and a user layer of OBUs.

The scheme is composed of two phases: offline registration phase and authentication phase in which each RSU authenticates a group of vehicles simultaneously as a batch which helps significantly in reducing the computation cost. Elliptic curve cryptography, one-way hash function, and bilinear pairing are utilized for generating secret key pairs and session keys during the offline registration phase and for securing communication during the authentication process. In the authentication phase, the shared session key of a vehicle is constructed independently which helps mitigate the interference in the regular V2R

data exchange. In addition, an efficient group key management mechanism that employs the Chinese Remainder Theorem (CRT) [138] is suggested by the authors for reliable and secure V2V communication. A consortium blockchain is deployed during the dynamic group key updating process to record the identity of the participating vehicles in order to provide traceability of vehicle's historical data when needed. Formal security analysis proves the resiliency of the proposed scheme to chosen message attacks and replay attacks. Low storage, communication, and computation overheads are also recorded through deep performance evaluation.

The authors in [139] designed a novel data structure based on the idea of the Unspent Transaction Output (UTXO) adopted in Bitcoin in combination with a group of online operations, namely, issue, transfer, query, and revocation. The system framework consists of two layers: the entity layer which is mainly the vehicles and RSUs that need authentication service and the trust layer represented by the TAs and the consortium blockchain. Each TA is responsible for managing a dedicated group of entities which all together form an organization. When creating a new block, a sufficient number of organizations must sign it to be accepted to the consortium blockchain. However, the authors developed the use of tokens in the UTXO to serve as a one-time guarantee for the authenticity of an entity instead of using incentives as in Bitcoin. Once an entity receives a token from another entity in the public ledger, this not only means an authentication request being issued, but also proves or guarantees the authenticity of the dedicated sender.

The UTXO data structure is formed by three key items, namely, basic, in, and out items. The basic item includes the transaction id, the operation name, the timestamp, and the signature of the requester to prove its ownership. The in item represents the information of the sending entity while the out item includes information related to the receiving entity. The authors define several operations that are as follows. The Issue operation is used by trusted authorities to generate new tokens for the entities, which can take place only upon two circumstances: the initial enrollment of a vehicle and periodically generated for well-behaved entities. Similarly, the Query operation can be used to retrieve the UTXO of a transaction on the blockchain through transaction id in order to check the trustworthiness of a sending entity. The Revoke operation is the key operation introduced by the authors for revocation management instead of the conventional certificate revocation list that implies extra storage and computation overheads. However, the main operation used for authentication purposes is the Transfer operation and the procedure is as follows: when an entity E_i sends an authentication request to Entity E_j, Entity E_j extracts the unique transaction id from the request message and uses it to query and retrieve the transaction UTXO from the blockchain. Then, the identities of the sending and receiving entities in the retrieved UTXO are compared against the ones received in the authentication request to check their legitimacy. If confirmed, the existence of the UTXO should be verified in the receiving entity's (E_j's) local database to check for token reuse. If the UTXO does not exist, the authentication is successful and it is recorded immediately in the database for future authentication references, otherwise, the authentication is rejected. In addition to resisting replay attacks (due to the use of timestamps and one-time tokens), the scheme prevents man-in-the-middle attack, identity revealing attack, as well as authority abuse attack.

The above-mentioned consortium blockchain-based authentication schemes can be found in Table 6 for the ready reference.

Table 6. A comparative study of the consortium blockchain-based authentication schemes in IoV and VANETs.

Ref.	Technique	Attack Counteracted	Network Model and Entities (Other than Blockchain)	Evaluation	Metrics	Features and Limitations	Privacy Preservation of Vehicle's Identity?
[128]	- Byzantine consensus mechanism - Gossip protocol and time sequence	Byzantine/faulty nodes attack	- V2I - Several VCNs - 5 RCNs - Data storage (multiple servers)	Mathematical modeling	Simple data comparisons	- Fast convergence speed. - Good Byzantine fault tolerance. - Good control over the entry/exit of multiple nodes to/from the network. - Lack of security analysis and performance evaluation.	No
[130]	- PBFT consensus mechanism - Asymmetric key crypto - Elliptic curve discrete logarithm problem	Impersonation	- V2I - OBUs - RSUs - Service managers - Witness peers - Audit department	- Simulation - Hardware components: OBU, RSU and SM represented by 3 PCs to measure the transmission delay	Time overhead (ms)	- Ensures Confidentiality and integrity of data. - Ensures traceability and non-repudiation of misbehaving vehicles. - Provides flexible cross-datacenter authentication. - Does not support mutual authentication. - Does not provide formal security analysis.	Yes
[131]	- PBFT consensus mechanism - Asymmetric key cryptography - Elliptic curve cryptography	- Impersonation - Replay	- V2I - OBUs - RSUs - Service managers - Witness peers - Audit department	- Automated Validation of Internet Security Protocols and Applications (AVISPA) simulation tool for formal security verification	- Computational overhead (ms) - Communication overhead	- Ensures confidentiality and integrity of data. - Ensures non-repudiation. - Supports non-interactivity, thus lightweight. - Supports forward secrecy. - Supports mutual authentication and key exchange. - Supports cross-datacenter authentication. - Does not discuss the details of the security analysis, i.e., threat model, assumptions, etc.	Yes
[132]	- PBFT consensus mechanism - Smart contract - Attribute-based Encryption - Elliptic curve cryptography - Fuzzy extractor	- Replay - Vehicle impersonation - Offline password guessing - DDoS	- V2I - The upper layer: Trusted authority (TA) - The bottom layer: RSUs and vehicles	- Software implementation using relic library for the time cost of the cryptographic operations - JavaScript on Hyperledger Fabric platform for the smart contract	Time overhead (5.693 s)	- Supports traceability and dynamic revocation of mis-behaving vehicles. - Does not evaluate the scheme in terms of communication overhead and storage overhead.	Yes

Table 6. *Cont.*

Ref.	Technique	Attack Counteracted	Network Model and Entities (Other than Blockchain)	Evaluation	Metrics	Features and Limitations	Privacy Preservation of Vehicle's Identity?
[133]	- PBFT consensus mechanism - Elliptic curve cryptography - One-way hash function	- DDoS - Replay - Man-in-the-middle - Identity theft - Traffic analysis - Masquerading - Session key disclosure	- V2V, V2I and V2R - Vehicles (OBUs) - RSUs - Trusted authority - Certification authority - Authentication manager - -Blockchain manager - Fog area	- Automated Validation of Internet Security Protocols and Applications (AVISPA) simulation tool and Random Oracle Model (ROM) - C++ software implementation under Visual Studio using Crypto++ library	- Computation overhead (91.04 ms) - Communication overhead (24 tokens) - Storage overhead (186 bytes)	- Guarantees the confidentiality and the integrity of data. - Guarantees traceability and non-repudiation. - Ensures perfect forward secrecy. - Supports non-interactivity. - Provides mutual authentication and key exchange.	Yes
[136]	Elliptic curve cryptography	Replay attacks	- V2I - OBUs - RSUs - TAs - Trusted cloud server - Traffic department	Not specified	- Time consumption (ms) - Storage capacity	- Ensures the confidentiality of data. - No single point of failure. - Reduces the computational overhead associated with vehicles' revocation. - Supports system scalability. - Insufficient evaluation.	Yes
[137]	- Elliptic curve crypto - Bilinear pairing - One-way hash	- Replay - Chosen message attack (CMA)	- V2V and V2R - Cloud server - RSUs - OBUs	- Their customized simulation	- Computation cost (ms) - Storage overhead (bits) - Communication cost (rounds)	- Provides efficient key updating that avoids the interference in V2R data exchange. - Provides efficient group key distribution scheme. - Conditional anonymity - Unforgeability - Formal security analysis is required.	Yes
[139]	- Smart contract - Public–private key pair cryptography	- Replay - Man-in-the-middle - Identity revealing - Authority abuse	- V2I - Vehicles - RSUs - Trusted authorities	- Testbed + Software implementation (a LAN of 4 nodes with a smart contract deployed over them)	- Time cost (ms) - Throughput (transactions per second)	- Reduced storage and computation overheads associated with the revocation process due to the discard of certificate revocation lists (CRLs). - Does not evaluate the scheme in terms of communication overhead and storage overhead.	Yes

5. Discussion

In Tables 4–6, we provide a summary of the blockchain-based authentication papers surveyed in Section 5. The table highlights the main properties of each scheme which are represented in the blockchain and cryptographic techniques used, the network model designed, the tools used for security verification and performance evaluation, the features, and limitations (if any), and whether each scheme supports a privacy preservation option for user's identity during the authentication process or not. From the table, we can conclude the following:

1. The choice of the consensus mechanism used by the blockchain depends on many factors such as the amount of power consumption the system can afford, the percentage of faulty nodes the network can tolerate, and others. However, the size of the IoV network is also an important factor to be considered. For example, although the PBFT consensus is lightweight in power consumption and has a good fault-tolerance of approximately 33%, it does not support high network scalability; thus, it is chosen only by the small-scale IoV platforms such as in [128], or by fog-based IoV networks where the whole network can be large but the consensus is performed in fog-area-basis such as in [123,130,131,133]. On the other hand, PoW has been chosen by the large-scale IoV environments [119,122,125,126] due to its high scalability and high fault tolerance, despite its large power consumption. In general, we can say that these two consensus mechanisms are the most commonly used by the blockchains when applied for IoV and VANETs authentication.
2. Some of the papers only considered a V2V model to investigate their authentication schemes such as [120], while most of them have considered an integrated network model (V2V and V2I). Due to the ad-hoc and mobile nature of V2V communication, the authentication is more challenging in it.
3. Most of the papers support anonymous authentication schemes, while some of them provide pure authentication without supporting such privacy preservation option as in [111,120,126,128].
4. In terms of performance analysis, the use of blockchain for authentication in IoV and VANETS networks introduces the need to include additional evaluation measures that reflect the efficiency of the blockchain itself such as the throughput which refers here to the number of transactions that can be verified and added to the blockchain per second [117,119,127,139], the transactions latency [119,122,127], and the blockchain storage overhead [123,126,133,136,137], beside other measures that are used commonly to evaluate the conventional cryptographic-based authentication schemes including the average packet delay, the average packet loss ratio, the communication cost, and the computational cost.
5. Regarding the security analysis, the different authentication schemes have shown uneven levels of resistance against the various security attacks introduced in the previous sections.

To conclude, a comprehensive view of the recent blockchain-assisted authentication schemes in IoV and VANETs was provided in this survey while highlighting the main differences between them in terms of security performance and operational performance. This helps in identifying the research gaps and creates a map that guides the future researchers in this area of IoV blockchain-based authentication. Although the adoption of blockchain for IoV authentication has brought many benefits such as the increased time-efficiency due to the decentralization of the authentication scheme among the distributed blockchain servers, and the more secure authentication reflected by the high resistance against different security attacks, a lot of work still must be done. This area needs more research and development to design new IoV-specific consensus mechanisms that can provide a more efficient balance between scalability and power consumption by consuming less power, supporting highly scalable IoV networks while maintaining the same good level of security represented by the high fault tolerance.

6. Future Research Directions and Open Challenges

In this section, a number of research challenges in IoV security that need to be addressed as well as some potential research directions to be explored are suggested.

6.1. Efficient Design of Blockchain-Assisted IoV Authentication

Despite the many advantages that blockchain technology has brought to the field of IoV authentication represented by a decentralized, autonomous, fault-tolerant, and more secured authentication protocols which are all properties that are required by any efficient authentication process, many challenges also arise with blockchains when being employed for authentication in environments with high performance expectations and critical security requirements such as the IoV. Most of these challenges are associated with the consensus mechanisms used by the blockchain, as different consensus protocols show uneven levels of support for the various IoV requirements such as scalability, fault tolerance, power consumption, as well as real-time response.

(1) Scalability: The scalability of a consensus mechanism depends on its way of reaching the consensus, whether it is Proof-based or Vote-based approach. Since Proof-based consensus protocols such as PoW and PoS do not require all the network entities to submit their individual decisions on the information to be verified, their scalability is not affected with more nodes being added to the network as at the end of the day they allocate the role of announcing the conclusions of all the participating nodes about the information to a single node. Thus, they can be suitable for large-scale networks such as the IoV environment. However, the huge amount of power consumed by these Proof-based consensus approaches undermines their efficiency and their suitability for all IoV environments especially the resource constrained ones. On the other hand, the Vote-based blockchain consensus making approaches such as the PBFT consensus mechanism exhibit negligible power consumption, yet their scalability is restricted to small-scale networks with limited number of nodes since all the nodes in the network are engaged in transaction verification and should submit their individual votes in order to reach consensus. For such a trade-off that is faced by the existing consensus mechanisms when employing blockchain for IoV, the challenge is represented in how to tune and improve these mechanisms in the future to be able to support efficient authentication in the highly scalable resource constrained IoV environments.

(2) Fault tolerance: the different blockchain consensus mechanisms have uneven capabilities in terms of how many faulty nodes each can tolerate while still being able to ensure the integrity of the participants and data in the network. In such wide and publicly opened environments as IoV where a variety of attacks can be encountered in which attackers impersonate the authentic nodes, high fault-tolerant consensus protocols should be adopted to ensure that the integrity of the communicated data can still be guaranteed even if the authenticity of a considerable percentage of participants is compromised. Some existing consensus protocols such as PoW can offer the high fault tolerance required for IoV environments; however, as discussed before it exhibits a large power consumption which can be an issue when used for authentication in some resource constrained IoV platforms. Thus, the need appears for developing new consensus making approaches that can guarantee high fault tolerance for the vulnerable IoV arrangements while maintaining an acceptable level of power consumption. Alternatively, mitigating the power consumption effect of the already existing blockchain consensus protocols by finding other solutions such as the charge-as-go solution represented by providing mobile charging units to charge the vehicles' batteries as they move to be able to tolerate the high power consumed during the authentication is a challenging proposal to be explored in the future.

(3) Communication mode: Due to the two types of communication used by the different consensus mechanisms which are synchronous and asynchronous communication modes, different time responses are expected. In the asynchronous mode, the sending entity does not wait for acknowledgement from the receiving node on a previous

request, instead, it directly proceeds with the following communication steps. The consensus protocols that use this mode of communication such as Proof of Work (PoW) and Proof of Time (PoT) could be thought of as perfectly suitable to be used for authentication in the different IoV applications which are mostly time-critical applications in which even a small delay of milli seconds is not forgivable. However, when considering some availability issues scenarios where the receiving entity can be temporarily out of network, waiting for an acknowledgement from the receiving entity before proceeding on with further interaction would save a lot of time and bandwidth that were used for such useless communication. Therefore, developing novel consensus making protocols that combine synchronous and asynchronous modes into one hybrid mode that incorporates the advantages of both communication modes, for example, by setting some thresholds for the number of acknowledgments to be received before proceeding the rest of communication asynchronously, or by using timeouts. However, such proposed solution is in turn full of challenges, since this hybrid mode of operation needs to be repeated periodically and regulated with other thresholds, that is, the synchronous mode should be injected once after every consecutive asynchronous interaction to check periodically that the receiving entity can be reached. This arrangement imposes an extra overhead associated with designing the optimal thresholds, monitoring, and managing the different time windows and timeouts. Thus, the feasibility of developing such complicated hybrid consensus protocols to be used for IoV authentication while maintaining a relatively low operational cost is another future challenge to be investigated.

Thus, to design an efficient authentication protocol for IoV based on blockchain that maintains a good performance balance while highly considering all the above-mentioned factors is a great challenge that should be addressed by future researchers. In the way to achieve this, serious efforts should be dedicated to developing all-in-one IoV-specific consensus mechanisms that can meet all the requirements of IoV applications including high scalability, high fault tolerance, real-time response with low energy consumption. Beside these factors, another important challenge in this area to consider is how to achieve the optimal assignment of the various blockchain-related tasks such as blocks creation, validation, and consensus making to the different IoV nodes based on their computing capabilities and the energy consumption requirements of the adopted consensus protocols in order to achieve an efficient authentication process. In [119] for instance, blocks creation is assigned to the infrastructure units through PoW due to their high computing power, whereas blocks verification is assigned to the vehicles through PBFT consensus due to their relatively low computing capabilities. However, more technical details and conditions need to be fully explored in upcoming research studies.

6.2. Employing Blockchain for other IoV Security Requirements

In this survey paper, we targeted the adoption of blockchain in IoV for the authentication security requirement. However, we believe that blockchain can be of great benefits for other IoV security requirements such as data integrity, secure routing, and availability which can all be explored and discussed as part of the future research directions.

(1) Data Integrity: Blockchain can be adopted by IoV environments to ensure that the data sent and received between two communicating IoV entities are identical. In other words, to make sure that no unauthorized modifications on the data take place during transmission. For instance, when a sender aims to send some data to another IoV node, it can send a copy of the data to the publicly accessible blockchain as well. At the other end, when the receiving entity receives the data, it can compare it with the copy stored in the immutable blockchain, if matched that means no manipulation was performed and data integrity is guaranteed. Otherwise, the received data cannot be trusted. The use of blockchains for ensuring data integrity in IoV may become even more important to explore when considering using them for big data analytics

and data mining which require the data to have high level of accuracy to result in developing accurate and efficient decision making and AI-based applications.

(2) Secure Routing: Blockchain technology can be used for guaranteeing a secure routing in IoV environments via different arrangements. An example could be maintaining a list of all possible legal next-hop nodes in the public ledger which can be accessed by all IoV entities. This list should be firstly developed by gradually adding the ids of the nodes that were successfully registered and authorized by the network. This means that any malicious unauthorized node will not be valid in this routing list. In this way, when an entity receives a packet that was routed through at least one illegal forwarder that does not exist in the routing list kept in the blockchain, this means the routing processes have been compromised and some illegal entity had access to the transmitted packet.

(3) Availability: A feasible suggestion that could be investigated is the integration of blockchain with some physical identification modules in an attempt to prevent some availability attacks and threats. That is, obligating each single service request to include the physical identity of the request originator, e.g., MAC address of the NIC of the user's mobile device or the vehicle's hardware id assigned by the vehicle manufacturer. Then, upon receiving the request by an infrastructure node, i.e., a RSU, it should extract the physical identity of the requester and store it as a record in the blockchain while keeping track of a counter that counts the number of successive requests and a timer to monitor the time intervals between these successive requests. In such arrangement, availability attacks specifically the denial of service (DoS) attack that originates from a single physical entity with different logical identities, i.e., IP addresses, can be efficiently detected and thus blocked by any IoV entity through monitoring the public ledger records and noticing any extraordinary behavior of rapid successive requests originated from the same physical id.

The above-mentioned examples are a few humble suggestions for using blockchain in the context of the different IoV security requirements. However, there is a strong belief that blockchain capabilities can cover more aspects and offer a variety of solutions regarding these IoV security concerns, yet to be explored.

6.3. Cloud Scalability, Security, and Privacy

Since IoV paradigm is based on big data and high-performance computing, cloud computing infrastructures constitute the most important building blocks for providing data storage. Even in blockchain-assisted IoV platforms, the cloud servers (CS) cluster constitutes the blockchain network.

Thus, developing the cloud technologies is a critical aspect to guarantee the security and the privacy of the blockchain-based authentication system in vehicular networks. Cloud-related security and privacy issues might be encountered during the process of transmitting vehicles' data to/from the cloud or while being stored in the different cloud servers. This imposes different security challenges in both processes which should be addressed in the future to guarantee a high level of efficiency for the blockchain-based cloud-assisted IoV authentication systems.

Data transmission challenges: Transmitting data back and forth between the cloud servers, the vehicles, and the other IoV entities via an open wireless network may impose high risks on the security of the blockchain-based authentication system and the privacy of the users. Some schemes attempt to mitigate the security risk by adopting wired communication wherever possible, i.e., between the cloud servers and the intermediate nodes. However, this arrangement is not practical nor feasible for all IoV-based scenarios. Moreover, this can only mitigate the risk at the stationary end of the system while the mobile part, i.e., the V2I communication is still exposed to different security threats due to its wireless nature. Thus, the existing wireless communication protocols should be well investigated and developed to insure private and secure exchange of users' authentication data between the different parts of the IoV-based system.

Data storage challenges: Having users' sensitive data such as the authentication data including users' real identities, public keys and certificates stored in a common-access platform such as the cloud is another threat to consider. The privacy of users is threatened to be violated if no proper encoding schemes exist within the cloud. Thus, the need for developing efficient encryption algorithms that can be adopted in both data storage and transmission to protect the privacy and security of the whole IoV cloud-based paradigm while ensuring full compatibility with the rapidly evolving and heterogenous cloud technologies is another important challenge which we hope to be tackled in the future.

7. Conclusions

In this survey, security aspects of the emerging vehicular technology, IoV, and the preceding VANETS which have made an evolution in the intelligent transportation systems were discussed. The power of the emerged blockchain technology in general and specifically in IoV was also highlighted. Moreover, different security requirements, challenges, and potential security attacks and threats in vehicular networks were presented. After that, more focus was dedicated to discussing a wide range of recent blockchain-based authentication techniques in IoV and VANETs environments and a comprehensive comparison between them was then provided. At last, some possible security challenges and research directions in IoV and VANETs that need to be addressed in the future were highlighted. In this paper, we focused only on the conceptual comparison between the surveyed blockchain-based IoV authentication schemes, i.e., in terms of the different techniques, network architectures, and evaluation tools used, as well as features and limitations. However, we believe that including more quantitative measures in comparisons is a direction that can be considered and improved in future surveys.

Author Contributions: Conceptualization, S.A.(Sohail Abbas), M.A.T. and A.A.; Data curation, S.A.(Sohail Abbas), M.A.T. and A.A.; Validation, S.A.(Sohail Abbas), M.A.T. and A.A.; Funding acquisition, F.K., S.A.(SHABIR AHMAD) and D.-H.K.; Investigation, F.K., S.A.(Sohail Abbas) and D.-H.K.; Methodology, S.A.(Sohail Abbas), M.A.T. and A.A.; Project administration, S.A.(Sohail Abbas) and M.A.T.; Resources, S.A.(Sohail Abbas), M.A.T., A.A., F.K., S.A.(Sohail Abbas) and D.-H.K.; Writing—original draft preparation, S.A.(Sohail Abbas), M.A.T. and A.A.; writing—review and editing, S.A.(Sohail Abbas), M.A.T., A.A., F.K., S.A.(Shabir Ahmad) and D.-H.K. All authors have read and agreed to the published version of the manuscript.

Funding: This research was supported by Energy Cloud R&D Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Science, ICT (2019M3F2A1073387), and this work was supported by Institute of Information & communications Technology Planning & Evaluation (IITP) grant funded by the Korea government (MSIT) (2021-0-00188, Open source development and standardization for AI enabled IoT platforms and interworking). Any correspondence related to this paper should be addressed to DoHyeun Kim.

Institutional Review Board Statement: Not Applicable.

Informed Consent Statement: Not Applicable.

Data Availability Statement: Not Applicable.

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

References

1. Chang, W.-J.; Chen, L.-B.; Su, K.-Y. DeepCrash: A deep learning-based Internet of vehicles system for head-on and single-vehicle accident detection with emergency notification. *IEEE Access* **2019**, *7*, 148163–148175. [CrossRef]
2. Dandala, T.T.; Krishnamurthy, V.; Alwan, R. Internet of Vehicles (IoV) for traffic management. In Proceedings of the 2017 International Conference on Computer, Communication and Signal Processing (ICCCSP), Chennai, India, 10–11 January 2017; pp. 1–4.
3. Vijayaraghavan, V.; Leevinson, J.R. Intelligent traffic management systems for next generation IoV in smart city scenario. In *Connected Vehicles in the Internet of Things*; Springer: Berlin/Heidelberg, Germany, 2020; pp. 123–141.
4. Khan, Z.; Koubaa, A.; Farman, H. Smart route: Internet-of-vehicles (iov)-based congestion detection and avoidance (iov-based cda) using rerouting planning. *Appl. Sci.* **2020**, *10*, 4541. [CrossRef]

5. Ang, L.-M.; Seng, K.P.; Ijemaru, G.K.; Zungeru, A.M. Deployment of IoV for smart cities: Applications, architecture, and challenges. *IEEE Access* **2018**, *7*, 6473–6492. [CrossRef]
6. Hamid, U.Z.A.; Zamzuri, H.; Limbu, D.K. Internet of vehicle (IoV) applications in expediting the implementation of smart highway of autonomous vehicle: A survey. In *Performability in Internet of Things*; Springer: Berlin/Heidelberg, Germany, 2019; pp. 137–157.
7. Sodhro, A.H.; Rodrigues, J.J.P.C.; Pirbhulal, S.; Zahid, N.; de Macedo, A.R.L.; de Albuquerque, V.H.C. Link optimization in software defined IoV driven autonomous transportation system. *IEEE Trans. Intell. Transp. Syst.* **2020**, *22*, 3511–3520. [CrossRef]
8. Yu, C.; Lin, B.; Guo, P.; Zhang, W.; Li, S.; He, R. Deployment and dimensioning of fog computing-based internet of vehicle infrastructure for autonomous driving. *IEEE Internet Things J.* **2018**, *6*, 149–160. [CrossRef]
9. Gupta, N.; Prakash, A.; Tripathi, R. *Internet of Vehicles and Its Applications in Autonomous Driving*; Springer: Berlin/Heidelberg, Germany, 2021; ISBN 3030463354.
10. Du, H.; Leng, S.; Wu, F.; Chen, X.; Mao, S. A new vehicular fog computing architecture for cooperative sensing of autonomous driving. *IEEE Access* **2020**, *8*, 10997–11006. [CrossRef]
11. Raja, G.; Dhanasekaran, P.; Anbalagan, S.; Ganapathisubramaniyan, A.; Bashir, A.K. SDN-enabled traffic alert system for IoV in smart cities. In Proceedings of the IEEE INFOCOM 2020-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), Toronto, ON, Canada, 6–9 July 2020; pp. 1093–1098.
12. Nouh, R.; Singh, M.; Singh, D. SafeDrive: Hybrid recommendation system architecture for early safety predication using Internet of Vehicles. *Sensors* **2021**, *21*, 3893. [CrossRef] [PubMed]
13. Chen, L.-W.; Chen, H.-M. Driver behavior monitoring and warning with dangerous driving detection based on the internet of vehicles. *IEEE Trans. Intell. Transp. Syst.* **2020**, *22*, 7232–7241. [CrossRef]
14. Hussain, R.; Kim, D.; Son, J.; Lee, J.; Kerrache, C.A.; Benslimane, A.; Oh, H. Secure and privacy-aware incentives-based witness service in social Internet of Vehicles clouds. *IEEE Internet Things J.* **2018**, *5*, 2441–2448. [CrossRef]
15. Xie, J.; Tang, H.; Huang, T.; Yu, F.R.; Xie, R.; Liu, J.; Liu, Y. A survey of blockchain technology applied to smart cities: Research issues and challenges. *IEEE Commun. Surv. Tutor.* **2019**, *21*, 2794–2830. [CrossRef]
16. Biswas, K.; Muthukkumarasamy, V. Securing smart cities using blockchain technology. In Proceedings of the IEEE 18th International Conference on High Performance Computing and Communications; IEEE 14th International Conference on Smart City; IEEE 2nd International Conference on Data Science and Systems (HPCC/SmartCity/DSS), Sydney, NSW, Australia, 12–14 December 2016; pp. 1392–1393.
17. Ibba, S.; Pinna, A.; Seu, M.; Pani, F.E. CitySense: Blockchain-oriented smart cities. In Proceedings of the XP2017 Scientific Workshops, Cologne, Germany, 22–26 May 2017; pp. 1–5.
18. Mollah, M.B.; Zhao, J.; Niyato, D.; Lam, K.-Y.; Zhang, X.; Ghias, A.M.Y.M.; Koh, L.H.; Yang, L. Blockchain for future smart grid: A comprehensive survey. *IEEE Internet Things J.* **2020**, *8*, 18–43. [CrossRef]
19. Wang, S.; Taha, A.F.; Wang, J.; Kvaternik, K.; Hahn, A. Energy crowdsourcing and peer-to-peer energy trading in blockchain-enabled smart grids. *IEEE Trans. Syst. Man Cybern. Syst.* **2019**, *49*, 1612–1623. [CrossRef]
20. Ferrag, M.A.; Maglaras, L. DeepCoin: A novel deep learning and blockchain-based energy exchange framework for smart grids. *IEEE Trans. Eng. Manag.* **2019**, *67*, 1285–1297. [CrossRef]
21. Koshy, P.; Babu, S.; Manoj, B.S. Sliding window blockchain architecture for internet of things. *IEEE Internet Things J.* **2020**, *7*, 3338–3348. [CrossRef]
22. Hassan, M.U.; Rehmani, M.H.; Chen, J. Privacy preservation in blockchain based IoT systems: Integration issues, prospects, challenges, and future research directions. *Futur. Gener. Comput. Syst.* **2019**, *97*, 512–529. [CrossRef]
23. Rathore, H.; Mohamed, A.; Guizani, M. A survey of blockchain enabled cyber-physical systems. *Sensors* **2020**, *20*, 282. [CrossRef]
24. Lee, J.; Azamfar, M.; Singh, J. A blockchain enabled Cyber-Physical System architecture for Industry 4.0 manufacturing systems. *Manuf. Lett.* **2019**, *20*, 34–39. [CrossRef]
25. Xu, Q.; Su, Z.; Yang, Q. Blockchain-based trustworthy edge caching scheme for mobile cyber-physical system. *IEEE Internet Things J.* **2019**, *7*, 1098–1110. [CrossRef]
26. Du, Y.; Cao, J.; Yin, J.; Song, S. An overview of blockchain-based swarm robotics system. *Artif. Intell. China* **2020**, *572*, 353–360.
27. Ferrer, E.C. The blockchain: A new framework for robotic swarm systems. In Proceedings of the Future Technologies Conference, Vancouver, BC, Canada, 13–14 November 2018; pp. 1037–1058.
28. Singh, S.; Sharma, P.K.; Yoon, B.; Shojafar, M.; Cho, G.H.; Ra, I.-H. Convergence of blockchain and artificial intelligence in IoT network for the sustainable smart city. *Sustain. Cities Soc.* **2020**, *63*, 102364. [CrossRef]
29. Chen, X.; Ji, J.; Luo, C.; Liao, W.; Li, P. When machine learning meets blockchain: A decentralized, privacy-preserving and secure design. In Proceedings of the 2018 IEEE International Conference on Big Data (Big Data), Seattle, WA, USA, 10–13 December 2018; pp. 1178–1187.
30. Wang, R.; Liu, H.; Wang, H.; Yang, Q.; Wu, D. Distributed security architecture based on blockchain for connected health: Architecture, challenges, and approaches. *IEEE Wirel. Commun.* **2019**, *26*, 30–36. [CrossRef]
31. Ramani, V.; Kumar, T.; Bracken, A.; Liyanage, M.; Ylianttila, M. Secure and efficient data accessibility in blockchain based healthcare systems. In Proceedings of the 2018 IEEE Global Communications Conference (GLOBECOM), Abu Dhabi, United Arab Emirates, 9–13 December 2018; pp. 206–212.

32. Wang, S.; Wang, J.; Wang, X.; Qiu, T.; Yuan, Y.; Ouyang, L.; Guo, Y.; Wang, F.-Y. Blockchain-powered parallel healthcare systems based on the ACP approach. *IEEE Trans. Comput. Soc. Syst.* **2018**, *5*, 942–950. [CrossRef]
33. Kang, J.; Yu, R.; Huang, X.; Wu, M.; Maharjan, S.; Xie, S.; Zhang, Y. Blockchain for secure and efficient data sharing in vehicular edge computing and networks. *IEEE Internet Things J.* **2018**, *6*, 4660–4670. [CrossRef]
34. Shi, K.; Zhu, L.; Zhang, C.; Xu, L.; Gao, F. Blockchain-based multimedia sharing in vehicular social networks with privacy protection. *Multimed. Tools Appl.* **2020**, *79*, 8085–8105. [CrossRef]
35. Li, Z.; Yang, Z.; Xie, S. Computing resource trading for edge-cloud-assisted Internet of Things. *IEEE Trans. Ind. Inform.* **2019**, *15*, 3661–3669. [CrossRef]
36. Qiao, G.; Leng, S.; Chai, H.; Asadi, A.; Zhang, Y. Blockchain empowered resource trading in mobile edge computing and networks. In Proceedings of the ICC 2019—2019 IEEE International Conference on Communications (ICC), Shanghai, China, 20–24 May 2019; pp. 1–6.
37. Chai, H.; Leng, S.; Zhang, K.; Mao, S. Proof-of-reputation based-consortium blockchain for trust resource sharing in internet of vehicles. *IEEE Access* **2019**, *7*, 175744–175757. [CrossRef]
38. Wang, S.; Huang, X.; Yu, R.; Zhang, Y.; Hossain, E. Permissioned blockchain for efficient and secure resource sharing in vehicular edge computing. *arXiv* **2019**, arXiv:1906.06319.
39. Al Amiri, W.; Baza, M.; Banawan, K.; Mahmoud, M.; Alasmary, W.; Akkaya, K. Privacy-preserving smart parking system using blockchain and private information retrieval. In Proceedings of the 2019 International Conference on Smart Applications, Communications and Networking (SmartNets), Sharm El Sheikh, Egypt, 17–19 December 2019; pp. 1–6.
40. Chen, C.; Xiao, T.; Qiu, T.; Lv, N.; Pei, Q. Smart-contract-based economical platooning in blockchain-enabled urban internet of vehicles. *IEEE Trans. Ind. Inform.* **2019**, *16*, 4122–4133. [CrossRef]
41. Li, M.; Zhu, L.; Lin, X. Efficient and privacy-preserving carpooling using blockchain-assisted vehicular fog computing. *IEEE Internet Things J.* **2018**, *6*, 4573–4584. [CrossRef]
42. Li, M.; Zhu, L.; Lin, X. CoRide: A privacy-preserving collaborative-ride hailing service using blockchain-assisted vehicular fog computing. In Proceedings of the International Conference on Security and Privacy in Communication Systems, Orlando, VA, USA, 23–25 October 2019; pp. 408–422.
43. Ren, Q.; Man, K.L.; Li, M.; Gao, B.; Ma, J. Intelligent design and implementation of blockchain and Internet of things–based traffic system. *Int. J. Distrib. Sens. Netw.* **2019**, *15*, 1550147719870653. [CrossRef]
44. Cheng, L.; Liu, J.; Xu, G.; Zhang, Z.; Wang, H.; Dai, H.-N.; Wu, Y.; Wang, W. SCTSC: A semicentralized traffic signal control mode with attribute-based blockchain in IoVs. *IEEE Trans. Comput. Soc. Syst.* **2019**, *6*, 1373–1385. [CrossRef]
45. Pourvahab, M.; Ekbatanifard, G. Digital forensics architecture for evidence collection and provenance preservation in iaas cloud environment using sdn and blockchain technology. *IEEE Access* **2019**, *7*, 153349–153364. [CrossRef]
46. 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]
47. Ferrag, M.A.; Maglaras, L.A.; Janicke, H.; Jiang, J.; Shu, L. Authentication protocols for internet of things: A comprehensive survey. *Secur. Commun. Netw.* **2017**, *2017*, 1–41. [CrossRef]
48. Manvi, S.S.; Tangade, S. A survey on authentication schemes in VANETs for secured communication. *Veh. Commun.* **2017**, *9*, 19–30. [CrossRef]
49. El-Hajj, M.; Fadlallah, A.; Chamoun, M.; Serhrouchni, A. A survey of internet of things (IoT) authentication schemes. *Sensors* **2019**, *19*, 1141. [CrossRef] [PubMed]
50. Ali, I.; Hassan, A.; Li, F. Authentication and privacy schemes for vehicular ad hoc networks (VANETs): A survey. *Veh. Commun.* **2019**, *16*, 45–61. [CrossRef]
51. Manivannan, D.; Moni, S.S.; Zeadally, S. Secure authentication and privacy-preserving techniques in Vehicular Ad-hoc NETworks (VANETs). *Veh. Commun.* **2020**, *25*, 100247. [CrossRef]
52. Bagga, P.; Das, A.K.; Wazid, M.; Rodrigues, J.J.P.C.; Park, Y. Authentication protocols in internet of vehicles: Taxonomy, analysis, and challenges. *IEEE Access* **2020**, *8*, 54314–54344. [CrossRef]
53. Kumar, S.; Velliangiri, S.; Karthikeyan, P.; Kumari, S.; Kumar, S.; Khan, M.K. A survey on the blockchain techniques for the Internet of Vehicles security. *Trans. Emerg. Telecommun. Technol.* **2021**, e4317. [CrossRef]
54. Wang, C.; Cheng, X.; Li, J.; He, Y.; Xiao, K. A survey: Applications of blockchain in the Internet of Vehicles. *Eurasip J. Wirel. Commun. Netw.* **2021**, *2021*, 1–16. [CrossRef]
55. Mendiboure, L.; Chalouf, M.A.; Krief, F. Survey on blockchain-based applications in internet of vehicles. *Comput. Electr. Eng.* **2020**, *84*, 106646. [CrossRef]
56. Contreras-Castillo, J.; Zeadally, S.; Guerrero-Ibañez, J.A. Internet of vehicles: Architecture, protocols, and security. *IEEE Internet Things J.* **2017**, *5*, 3701–3709. [CrossRef]
57. Kaiwartya, O.; Abdullah, A.H.; Cao, Y.; Altameem, A.; Prasad, M.; Lin, C.-T.; Liu, X. Internet of vehicles: Motivation, layered architecture, network model, challenges, and future aspects. *IEEE Access* **2016**, *4*, 5356–5373. [CrossRef]
58. Ji, B.; Zhang, X.; Mumtaz, S.; Han, C.; Li, C.; Wen, H.; Wang, D. Survey on the internet of vehicles: Network architectures and applications. *IEEE Commun. Stand. Mag.* **2020**, *4*, 34–41. [CrossRef]
59. Xu, C.; Liu, H.; Zhang, Y.; Wang, P. Mutual authentication for vehicular network in complex and uncertain driving. *Neural Comput. Applic.* **2020**, *32*, 61–72. [CrossRef]

60. Yang, F.; Li, J.; Lei, T.; Wang, S. Architecture and key technologies for Internet of Vehicles: A survey. *J. Commun. Inf. Netw.* **2017**, *2*, 1–17. [CrossRef]
61. Alouache, L.; Nguyen, N.; Aliouat, M.; Chelouah, R. Toward a hybrid SDN architecture for V2V communication in IoV environment. In Proceedings of the 2018 Fifth International Conference on Software Defined Systems (SDS), Barcelona, Spain, 23–26 April 2018; pp. 93–99.
62. Contreras-Castillo, J.; Zeadally, S.; Guerrero Ibáñez, J.A. A seven-layered model architecture for Internet of Vehicles. *J. Inf. Telecommun.* **2017**, *1*, 4–22. [CrossRef]
63. Darwish, T.S.J.; Bakar, K.A. Fog based intelligent transportation big data analytics in the internet of vehicles environment: Motivations, architecture, challenges, and critical issues. *IEEE Access* **2018**, *6*, 15679–15701. [CrossRef]
64. Aggarwal, S.; Chaudhary, R.; Aujla, G.S.; Kumar, N.; Choo, K.-K.R.; Zomaya, A.Y. Blockchain for smart communities: Applications, challenges and opportunities. *J. Netw. Comput. Appl.* **2019**, *144*, 13–48. [CrossRef]
65. Raikwar, M.; Gligoroski, D.; Kralevska, K. SoK of used cryptography in blockchain. *IEEE Access* **2019**, *7*, 148550–148575. [CrossRef]
66. Zhai, S.; Yang, Y.; Li, J.; Qiu, C.; Zhao, J. Research on the application of cryptography on the blockchain. *J. Phys. Conf. Ser.* **2019**, *1168*, 32077. [CrossRef]
67. Zhang, S.; Lee, J.H. Analysis of the main consensus protocols of blockchain. *ICT Express* **2020**, *6*, 93–97. [CrossRef]
68. Zheng, Z.; Xie, S.; Dai, H.; Chen, X.; Wang, H. An overview of blockchain technology: Architecture, consensus, and future trends. In Proceedings of the 2017 IEEE 6th International Congress on Big Data, BigData Congress 2017, Honolulu, HI, USA, 25–30 June 2017; pp. 557–564.
69. Wazid, M.; Das, A.K.; Shetty, S.; Jo, M. A tutorial and future research for building a blockchain-based secure communication scheme for internet of intelligent things. *IEEE Access* **2020**, *8*, 88700–88716. [CrossRef]
70. Mollah, M.B.; Zhao, J.; Niyato, D.; Guan, Y.L.; Yuen, C.; Sun, S.; Lam, K.Y.; Koh, L.H. Blockchain for the internet of vehicles towards intelligent transportation systems: A survey. *IEEE Internet Things J.* **2021**, *8*, 4157–4185. [CrossRef]
71. Viriyasitavat, W.; Hoonsopon, D. Blockchain characteristics and consensus in modern business processes. *J. Ind. Inf. Integr.* **2019**, *13*, 32–39. [CrossRef]
72. Begicheva, A.; Kofman, A. Fair proof of stake. *Tech. Rep.* **2018**, 1–13. [CrossRef]
73. Kumar, M.A.; Radhesyam, V.; Srinivasarao, B. Front-End IoT application for the bitcoin based on proof of elapsed time (PoET). In Proceedings of the 3rd International Conference on Inventive Systems and Control, ICISC 2019, Coimbatore, India, 10–11 January 2019; pp. 646–649.
74. Liu, Z.; Tang, S.; Chow, S.S.M.; Liu, Z.; Long, Y. Fork-free hybrid consensus with flexible Proof-of-Activity. *Futur. Gener. Comput. Syst.* **2019**, *96*, 515–524. [CrossRef]
75. NEM, T. Nem Technical Reference. 2018. Available online: https//nem.io/wpcontent/themes/nem/files/NEM_techRef.pdf (accessed on 18 June 2021).
76. Jiang, S.; Wu, J. A game-theoretic approach to storage offloading in PoC-based mobile blockchain mining. *Proc. Int. Symp. Mob. Ad Hoc Netw. Comput.* **2020**, *1*, 171–180. [CrossRef]
77. Karantias, K.; Kiayias, A.; Zindros, D. *Proof-of-Burn BT—Financial Cryptography and Data Security*; Springer: Berlin/Heidelberg, Germany, 2020; pp. 523–540.
78. Li, K.; Li, H.; Hou, H.; Li, K.; Chen, Y. Proof of vote: A high-performance consensus protocol based on vote mechanism & consortium blockchain. In Proceedings of the IEEE 19th Intl Conference on High Performance Computing and Communications, HPCC 2017, IEEE 15th Intl Conference on Smart City, SmartCity 2017 and IEEE 3rd Intl Conference on Data Science and Systems, DSS, Bangkok, Thailand, 18–20 December 2017; pp. 466–473.
79. Niranjanamurthy, M.; Nithya, B.N.; Jagannatha, S. Analysis of blockchain technology: Pros, cons and SWOT. *Clust. Comput.* **2019**, *22*, 14743–14757. [CrossRef]
80. Vujičić, D.; Jagodić, D.; Ranđić, S. Blockchain technology, bitcoin, and Ethereum: A brief overview. In Proceedings of the 2018 17th International Symposium Infoteh-Jahorina (Infoteh), East Sarajevo, Bosnia and Herzegovina, 21–23 March 2018; pp. 1–6.
81. Lee, X.T.; Khan, A.; Sen Gupta, S.; Ong, Y.H.; Liu, X. Measurements, analyses, and insights on the entire ethereum blockchain network. In Proceedings of the Web Conference 2020, New York, NY, USA, 20–24 April 2020; pp. 155–166.
82. Cachin, C. Architecture of the hyperledger blockchain fabric. In Proceedings of the Workshop on Distributed Cryptocurrencies and Consensus Ledgers, Chicago, IL, USA, 25 July 2016; Volume 310.
83. Benji, M.; Sindhu, M. A study on the Corda and Ripple blockchain platforms. In *Advances in Big Data and Cloud Computing*; Springer: Berlin/Heidelberg, Germany, 2019; pp. 179–187.
84. Liu, M.; Wu, K.; Xu, J.J. How will blockchain technology impact auditing and accounting: Permissionless versus permissioned blockchain. *Curr. Issues Audit.* **2019**, *13*, A19–A29. [CrossRef]
85. Tripathi, G.; Ahad, M.A.; Sathiyanarayanan, M. The Role of Blockchain in Internet of Vehicles (IoV): Issues, challenges and opportunities. In Proceedings of the 2019 International Conference on contemporary Computing and Informatics (IC3I), Singapore, 12–14 December 2019; pp. 26–31.
86. Ali, M.S.; Vecchio, M.; Pincheira, M.; Dolui, K.; Antonelli, F.; Rehmani, M.H. Applications of blockchains in the internet of things: A comprehensive survey. *IEEE Commun. Surv. Tutor.* **2019**, *21*, 1676–1717. [CrossRef]
87. Hasrouny, H.; Samhat, A.E.; Bassil, C.; Laouiti, A. VANet security challenges and solutions: A survey. *Veh. Commun.* **2017**, *7*, 7–20. [CrossRef]

88. Qureshi, K.N.; Din, S.; Jeon, G.; Piccialli, F. Internet of vehicles: Key technologies, network model, solutions and challenges with future aspects. *IEEE Trans. Intell. Transp. Syst.* **2021**, *22*, 1777–1786. [CrossRef]
89. Sharma, S.; Kaushik, B. A survey on internet of vehicles: Applications, security issues & solutions. *Veh. Commun.* **2019**, *20*, 100182. [CrossRef]
90. Garg, T.; Kagalwalla, N.; Churi, P.; Pawar, A.; Deshmukh, S. A survey on security and privacy issues in IoV. *Int. J. Electr. Comput. Eng.* **2020**, *10*, 5409–5419. [CrossRef]
91. Abu Talib, M.; Abbas, S.; Nasir, Q.; Mowakeh, M.F. Systematic literature review on Internet-of-Vehicles communication security. *Int. J. Distrib. Sens. Netw.* **2018**, *14*. [CrossRef]
92. Abdus, S.; Shadab, A.; Mohammed, S.; Bokhari, M.U. Internet of Vehicles (IoV) requirements, attacks and countermeasures. In Proceedings of the 5 International Conference on "Computing for Sustainable Global Development", New Delhi, India, 14–16 March 2018; pp. 4037–4040.
93. Sun, Y.; Wu, L.; Wu, S.; Li, S.; Zhang, T.; Zhang, L.; Xu, J.; Xiong, Y.; Cui, X. Attacks and countermeasures in the internet of vehicles. *Ann. Telecommun.* **2017**, *72*, 283–295. [CrossRef]
94. Sun, Y.; Wu, L.; Wu, S.; Li, S.; Zhang, T.; Zhang, L.; Xu, J.; Xiong, Y. Security and privacy in the internet of vehicles. In Proceedings of the 2015 International Conference on Identification, Information, and Knowledge in the Internet of Things (IIKI), Beijing, China, 22–23 October 2015; pp. 116–121.
95. Qu, F.; Wu, Z.; Wang, F.-Y.; Cho, W. A security and privacy review of VANETs. *IEEE Trans. Intell. Transp. Syst.* **2015**, *16*, 2985–2996. [CrossRef]
96. Aouzellag, H.; Ghedamsi, K.; Aouzellag, D. Energy management and fault tolerant control strategies for fuel cell/ultra-capacitor hybrid electric vehicles to enhance autonomy, efficiency and life time of the fuel cell system. *Int. J. Hydrogen Energy* **2015**, *40*, 7204–7213. [CrossRef]
97. Wu, W.; Yang, Z.; Li, K. Internet of Vehicles and applications. In *Internet of Things*; Elsevier: Amsterdam, The Netherlands, 2016; pp. 299–317.
98. Al-Jarrah, O.Y.; Maple, C.; Dianati, M.; Oxtoby, D.; Mouzakitis, A. Intrusion detection systems for intra-vehicle networks: A review. *IEEE Access* **2019**, *7*, 21266–21289. [CrossRef]
99. Sakiz, F.; Sen, S. A survey of attacks and detection mechanisms on intelligent transportation systems: VANETs and IoV. *Ad Hoc Netw.* **2017**, *61*, 33–50. [CrossRef]
100. Hao, Y.; Tang, J.; Cheng, Y. Cooperative Sybil attack detection for position based applications in privacy preserved VANETs. In Proceedings of the 2011 IEEE Global Telecommunications Conference-GLOBECOM 2011, Houston, TX, USA, 5–9 December 2011; pp. 1–5.
101. Lee, B.; Jeong, E.; Jung, I. A DTSA (detection technique against a sybil attack) protocol using SKC (session key based certificate) on VANET. *Int. J. Secur. Its Appl.* **2013**, *7*, 1–10.
102. Feng, X.; Li, C.; Chen, D.; Tang, J. A method for defensing against multi-source Sybil attacks in VANET. *Peer-to-Peer Netw. Appl.* **2017**, *10*, 305–314. [CrossRef]
103. Chang, S.; Qi, Y.; Zhu, H.; Zhao, J.; Shen, X. Footprint: Detecting Sybil attacks in urban vehicular networks. *IEEE Trans. Parallel Distrib. Syst.* **2012**, *23*, 1103–1114. [CrossRef]
104. Studer, A.; Luk, M.; Perrig, A. Efficient mechanisms to provide convoy member and vehicle sequence authentication in VANETs. In Proceedings of the 2007 Third International Conference on Security and Privacy in Communications Networks and the Workshops-SecureComm 2007, Nice, France, 17–21 September 2007; pp. 422–432.
105. He, L.; Zhu, W.T. Mitigating DoS attacks against signature-based authentication in VANETs. In Proceedings of the 2012 IEEE International Conference on Computer Science and Automation Engineering (CSAE), Zhangjiajie, China, 25–27 May 2012; Volume 3, pp. 261–265.
106. Al-Kahtani, M.S. Survey on security attacks in vehicular ad hoc networks (VANETs). In Proceedings of the 2012 6th International Conference on Signal Processing and Communication Systems, Gold Coast, Australia, 12–14 December 2012; pp. 1–9.
107. Xie, Y.; Wu, L.; Shen, J.; Alelaiwi, A. EIAS-CP: New efficient identity-based authentication scheme with conditional privacy-preserving for VANETs. *Telecommun. Syst.* **2017**, *65*, 229–240. [CrossRef]
108. Safi, S.M.; Movaghar, A.; Mohammadizadeh, M. A novel approach for avoiding wormhole attacks in VANET. In Proceedings of the 2009 Second International Workshop on Computer Science and Engineering, Qingdao, China, 28–30 October 2009; Volume 2, pp. 160–165.
109. Biswas, S.; Mišić, J. A cross-layer approach to privacy-preserving authentication in WAVE-enabled VANETs. *IEEE Trans. Veh. Technol.* **2013**, *62*, 2182–2192. [CrossRef]
110. Adjih, C.; Raffo, D.; Muhlethaler, P. Attacks against OLSR: Distributed key management for security. In Proceedings of the 2nd OLSR Interop/Workshop, Palaiseau, France, 28 August 2005; Volume 14, pp. 1–5.
111. Wang, X.; Zeng, P.; Patterson, N.; Jiang, F.; Doss, R. An improved authentication scheme for internet of vehicles based on blockchain technology. *IEEE Access* **2019**, *7*, 45061–45072. [CrossRef]
112. Xu, Z.; Liang, W.; Li, K.C.; Xu, J.; Jin, H. A blockchain-based Roadside Unit-assisted authentication and key agreement protocol for Internet of Vehicles. *J. Parallel Distrib. Comput.* **2021**, *149*, 29–39. [CrossRef]
113. Yang, F.; Zhou, W.; Wu, Q.; Long, R.; Xiong, N.N.; Zhou, M. Delegated proof of stake with downgrade: A secure and efficient blockchain consensus algorithm with downgrade mechanism. *IEEE Access* **2019**, *7*, 118541–118555. [CrossRef]

114. Blanchet, B. *Proverif Automatic Cryptographic Protocol Verifier User Manual*; CNRS: Paris, France; Departement dInformatique, Ecole Normale Superieure: Paris, France, 2005.
115. Sharma, R.; Chakraborty, S. BlockAPP: Using blockchain for authentication and privacy preservation in IoV. In Proceedings of the IEEE Globecom Workshops (GC Wkshps), Abu Dhabi, United Arab Emirates, 9–13 December 2018; pp. 1–6. [CrossRef]
116. Ahirwal, R.R.; Ahke, M. Elliptic curve diffie-hellman key exchange algorithm for securing hypertext information on wide area network. *Int. J. Comput. Sci. Inf. Technol.* **2013**, *4*, 363–368.
117. Malik, N.; Nanda, P.; Arora, A.; He, X.; Puthal, D. Blockchain based secured identity authentication and expeditious revocation framework for vehicular networks. In Proceedings of the 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications and 12th IEEE International Conference on Big Data Science and Engineering, Trustcom/BigDataSE, New York, NY, USA, 1–3 August 2018; pp. 674–679. [CrossRef]
118. Khalique, A.; Singh, K.; Sood, S. Implementation of elliptic curve digital signature algorithm. *Int. J. Comput. Appl.* **2010**, *2*, 21–27. [CrossRef]
119. Noh, J.; Jeon, S.; Cho, S. Distributed blockchain-based message authentication scheme for connected vehicles. *Electronics* **2020**, *9*, 74. [CrossRef]
120. Kamal, M.; Srivastava, G.; Tariq, M. Blockchain-based lightweight and secured V2V communication in the internet of vehicles. *IEEE Trans. Intell. Transp. Syst.* **2020**, *22*, 3997–4004. [CrossRef]
121. Benesty, J.; Chen, J.; Huang, Y.; Cohen, I. Pearson correlation coefficient. In *Noise Reduction in Speech Processing*; Springer: Berlin/Heidelberg, Germany, 2009; pp. 1–4.
122. Javaid, U.; Aman, M.N.; Sikdar, B. A scalable protocol for driving trust management in internet of vehicles with blockchain. *IEEE Internet Things J.* **2020**, *7*, 11815–11829. [CrossRef]
123. Bagga, P.; Sutrala, A.K.; Das, A.K.; Vijayakumar, P. Blockchain-based batch authentication protocol for Internet of Vehicles. *J. Syst. Archit.* **2021**, *113*, 101877. [CrossRef]
124. Vangala, A.; Bera, B.; Saha, S.; Das, A.K.; Kumar, N.; Park, Y.H. Blockchain-enabled certificate-based authentication for vehicle accident detection and notification in intelligent transportation systems. *IEEE Sens. J.* **2020**, *1748*, 15824–15838. [CrossRef]
125. Lin, C.; He, D.; Huang, X.; Kumar, N.; Choo, K.-K.R. BCPPA: A blockchain-based conditional privacy-preserving authentication protocol for vehicular ad hoc networks. *IEEE Trans. Intell. Transp. Syst.* **2020**, 1–13. [CrossRef]
126. Ma, Z.; Zhang, J.; Guo, Y.; Liu, Y.; Liu, X.; He, W. An efficient decentralized key management mechanism for VANET with blockchain. *IEEE Trans. Veh. Technol.* **2020**, *69*, 5836–5849. [CrossRef]
127. Lu, Z.; Wang, Q.; Qu, G.; Zhang, H.; Liu, Z. A blockchain-based privacy-preserving authentication scheme for VANETs. *IEEE Trans. Very Large Scale Integr. Syst.* **2019**, *27*, 2792–2801. [CrossRef]
128. Hu, W.; Hu, Y.; Yao, W.; Li, H. A blockchain-based byzantine consensus algorithm for information authentication of the internet of vehicles. *IEEE Access* **2019**, *7*, 139703–139711. [CrossRef]
129. Cooper, M.C.; Herzig, A.; Maffre, F.; Maris, F.; Régnier, P. The epistemic gossip problem. *Discrete Math.* **2019**, *342*, 654–663. [CrossRef]
130. Yao, Y.; Chang, X.; Misic, J.; Misic, V.B.; Li, L. BLA: Blockchain-assisted lightweight anonymous authentication for distributed vehicular fog services. *IEEE Internet Things J.* **2019**, *6*, 3775–3784. [CrossRef]
131. Kaur, K.; Garg, S.; Kaddoum, G.; Gagnon, F.; Ahmed, S.H. Blockchain-based lightweight authentication mechanism for vehicular fog infrastructure. *arXiv* **2019**, arXiv:1904.01168v1, 2019, 1–6, 1–6.
132. Feng, Q.; He, D.; Zeadally, S.; Liang, K. BPAS: Blockchain-assisted privacy-preserving authentication system for vehicular ad hoc networks. *IEEE Trans. Ind. Inform.* **2020**, *16*, 4146–4155. [CrossRef]
133. Salah, M.; Amine, M.; Friha, O.; Maglaras, L. EASBF: An efficient authentication scheme over blockchain for fog computing-enabled internet of vehicles. *J. Inf. Secur. Appl.* **2021**, *59*, 102802.
134. Koblitz, N.; Menezes, A.J. The random oracle model: A twenty-year retrospective. *Des. Codes Cryptogr.* **2015**, *77*, 587–610. [CrossRef]
135. Armando, A.; Basin, D.; Boichut, Y.; Chevalier, Y.; Compagna, L.; Cuéllar, J.; Drielsma, P.H.; Héam, P.-C.; Kouchnarenko, O.; Mantovani, J. The AVISPA tool for the automated validation of internet security protocols and applications. In Proceedings of the International Conference on Computer Aided Verification, Edinburgh, UK, 6–10 July 2005; Springer: Berlin/Heidelberg, Germany, 2005; pp. 281–285.
136. Wang, L.; Zheng, D.; Guo, R.; Hu, C.; Jing, C. A blockchain-based privacy-preserving authentication scheme with anonymous identity in vehicular networks. *Int. J. Netw. Secur.* **2020**, *22*, 981–990. [CrossRef]
137. Tan, H.; Chung, I. Secure authentication and key management with blockchain in VANETs. *IEEE Access* **2020**, *8*, 2482–2498. [CrossRef]
138. Pei, D.; Salomaa, A.; Ding, C. *Chinese Remainder Theorem: Applications in Computing, Coding, Cryptography*; World Scientific: Singapore, 1996; ISBN 981449836X.
139. Zhang, Y.; Tong, F.; Xu, Y.; Tao, J.; Cheng, G. A privacy-preserving authentication scheme for VANETs based on consortium blockchain. In Proceedings of the 2020 IEEE 92nd Vehicular Technology Conference (VTC2020-Fall), Victoria, BC, Canada, 18 November–16 December 2020. [CrossRef]