Blockchain-Based Authentication in Internet of Vehicles

Subjects: Computer Science, Artificial Intelligence
Contributor: Sohail Abbas

Internet of Vehicles (IoV) is capable of providing various intelligent services and supporting different applications for the drivers and passengers on roads. The IoV to be able to offer beneficial road services, huge amounts of data are generated and exchanged among the different communicated entities wirelessly via open channels, which could attract the adversaries and threaten the network with several possible types of security attacks. In this survey, the authentication part of security system is targeted while highlighting the efficiency of blockchains in the IoV environments.

Keywords: authentication ; blockchain ; Internet of Vehicles ; vehicular ad-hoc network

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][3][4], evolution of smart cities [5][6], autonomous driving [7][8][9][10] alarms and dynamic warning systems [11][12][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][16][17], smart grids [18][19][20], Internet of Things (IoT) [21][22], Cyber Physical Systems (CPS) [23][24][25], robotics [26][27], machine learning [28][29], and health systems [30][31][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.
[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.

Ref.	Year	Target Area	VANETs to IoV Transition	Security Attacks and/or Requirements	Blockchain-Based Authentication	Features
[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.
[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.

Ref.	Year	Target Area	VANETs to IoV Transition	Security Attacks and/or Requirements	Blockchain-Based Authentication	Features
[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.

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]:

- 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.
- 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.
- Despite the rapid technological advancement of personal mobile devices, they could not communicate with VANETs due to the incompatible network architecture.
- 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.

- 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].

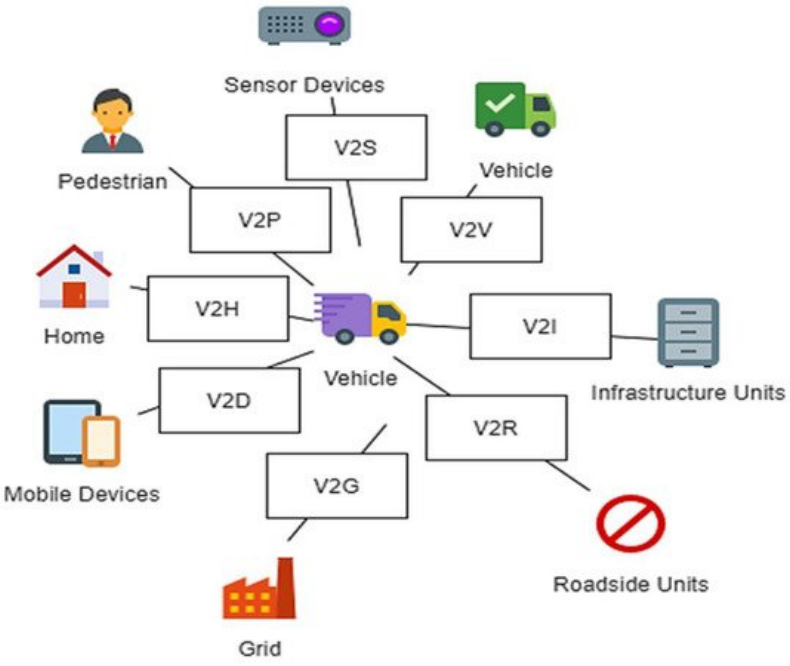

Figure 1. Communication models in IoV.

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][61][62][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.

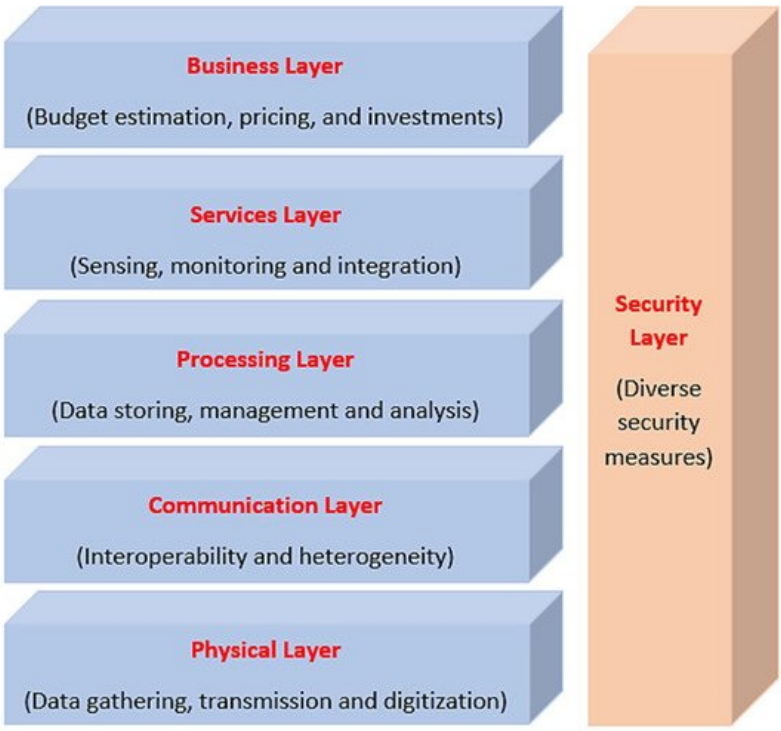

Figure 2. The proposed six-layers architecture of IoV.

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][65][66] and consensus mechanisms [67][68][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][80][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]:

- 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.

- 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.

- 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.

- 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.

- 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.

- 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.

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][88][89][90][91]:

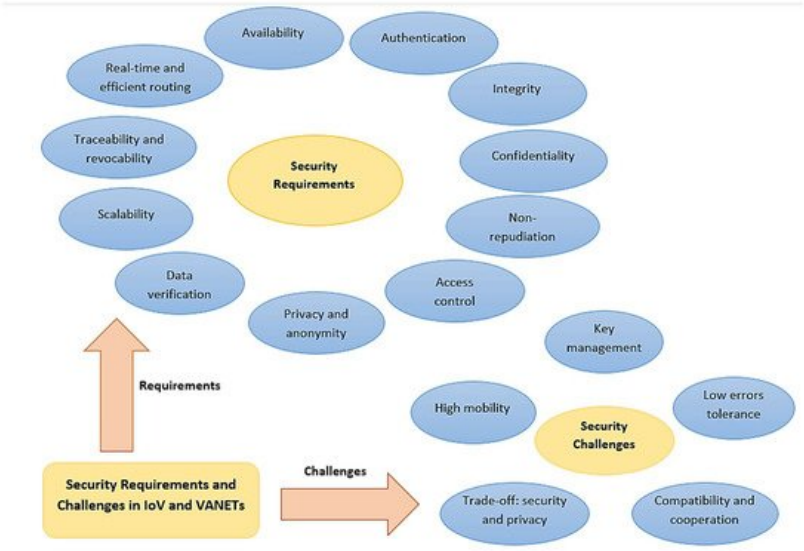

Figure 3. The security requirements and challenges in IoV and VANETs platforms.

- 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.

- 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.

- 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.

- 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.

- 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.

- 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.

- 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.

- 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.

- 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.

- 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.

- 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.

The following are different security challenges that might be faced by any IoV paradigm [89][92][93][94][95][96][97]:

- 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.

- 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.

- 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.

- 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.

- 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.

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.
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.
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.
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.
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.
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.
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.
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.
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.
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.

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.
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.
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.
21. Koshy, P.; Babu, S.; Manoj, B.S. Sliding window blockchain architecture for internet of things. IEEE Internet Things J. 2020, 7, 3338–3348.
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.
23. Rathore, H.; Mohamed, A.; Guizani, M. A survey of blockchain enabled cyber-physical systems. Sensors 2020, 20, 282.
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.
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.
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.
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.
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.
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.
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.
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.
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.
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.
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.
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.
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.
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.
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.
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.
48. Manvi, S.S.; Tangade, S. A survey on authentication schemes in VANETs for secured communication. Veh. Commun. 2017, 9, 19–30.
49. El-Hajj, M.; Fadlallah, A.; Chamoun, M.; Serhrouchni, A. A survey of internet of things (IoT) authentication schemes. Sensors 2019, 19, 1141.
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.
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.
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.
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.
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.
55. Mendiboure, L.; Chalouf, M.A.; Krief, F. Survey on blockchain-based applications in internet of vehicles. Comput. Electr. Eng. 2020, 84, 106646.
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.
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.
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.
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.
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.
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.

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.
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.
65. Raikwar, M.; Gligoroski, D.; Kralevska, K. SoK of used cryptography in blockchain. IEEE Access 2019, 7, 148550–148575.
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.
67. Zhang, S.; Lee, J.H. Analysis of the main consensus protocols of blockchain. ICT Express 2020, 6, 93–97.
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.
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.
71. Viriyasitavat, W.; Hoonsopon, D. Blockchain characteristics and consensus in modern business processes. J. Ind. Inf. Integr. 2019, 13, 32–39.
72. Begicheva, A.; Kofman, A. Fair proof of stake. Tech. Rep. 2018, 1–13.
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.
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.
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.
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.
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.
87. Hasrouny, H.; Samhat, A.E.; Bassil, C.; Laouiti, A. VANet security challenges and solutions: A survey. Veh. Commun. 2017, 7, 7–20.
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.
89. Sharma, S.; Kaushik, B. A survey on internet of vehicles: Applications, security issues & solutions. Veh. Commun. 2019, 20, 100182.
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.
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.
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.
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.
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.
97. Wu, W.; Yang, Z.; Li, K. Internet of Vehicles and applications. In Internet of Things; Elsevier: Amsterdam, The Netherlands, 2016; pp. 299–317.
