Blockchain-Enabled Vehicular Ad Hoc Networks

Subjects: Computer Science, Hardware & Architecture

Contributor: Muhammad Saad , Maaz Ahmad , Maaz Bin Ahmad

Within the paradigm of distributed ledger technology (DLT), the communication models and practices for vehicular ad hoc networks (VANETs) have been revolutionized. VANETs introduce a network of self-organizing vehicles that act as mobile nodes. They confine the communication between vehicles and roadside units as V2V and V2R. They assists drivers in avoiding collisions, picking the shortest route on the basis of traffic optimization, identifying tolls and the nearest fuel stations, and in enhancing the safety of assets and lives. They facilitate the communication of vehicles across the network for real-time data transmission. They improve the road safety mechanism and provide instant alerts or information in order to concern the authorities in cases of emergency situations, such as rollovers, accidents, etc. The existing architecture of VANETs also exposes vulnerabilities, such as data sniffing, impersonation, and ransomware attacks.

blockchain distributed ledger technology Internet of Things vehicular ad hoc networks vanets internet of vehicles M2M LTE Fleet Management Journey Management

1. Introduction

A blockchain is the extended form of a decentralized network that is responsible for recording transactional data or information in the form of blocks that are sequentially linked to each other. The architecture of blockchain makes it difficult to tamper with and difficult to modify information without having a consensus mechanism. In 2008, blockchain technology emerged with the revolution in digital currency known as âbitcoinâ. The blockchain network provides immutability, security, transparency, and reliability. Therefore, the inherent characteristics of blockchain technology are being recognized by practitioners for their implementation in different sectors. The integration of blockchain technology with other domains helps to overcome the privacy and security limitations by providing a tamper-proof network system. For example, an intelligent transportation system heavily relies on information sharing across multiple entities. The open-channel information sharing presents several security issues, such as denial-of-service attack (DDoS), man-in-the-middle attacks, etc. The application of blockchain technology can make this information tamper-proof, transparent, and reliable. Similarly, it can be applied to the Internet of Things (IoT) and the Internet of Vehicles (IoV), as well as to other domains where secure data transmission is required.

In recent years, several studies, discussions, and projects regarding blockchain have been recognized by researchers. The concept of blockchain is based on distributed ledger technology (DLT), which delivers a radical change to the existing trust model in order to overcome the limitations of centralized systems, and which provides an efficient data-trading mechanism. The conventional business processes are highly dependent on centralized systems (e.g., banks) to develop trust across the participants [1][2]. However, the centralized system always remains vulnerable to multiple attacks. Researchers have published several studies with the aim of mitigating the artificial alterations to the system using blockchain. The blockchain architecture that is based on trust is proposed by researchers to prevent security attacks, including Sybil, DDoS, and MAC layer attacks [3]. The challenge of security is one of the key areas of research in the realm of blockchain and its applications. Business operations and activities can be made

secure, transparent, and immutable by using the emerging blockchain technology. The immutable, decentralized, and distributed characteristics of blockchain also bring innovation to other technologies as composite uses of DLT [4].

Blockchain is considered to be a connected chain of sequential blocks. Each individual block represents the record of a digital transaction that is secured using cryptographic techniques. A peer-to-peer network (P2P) assists in creating the blocks, along with their validation, and the consensus is achieved by having majority votes in a blockchain network. This method provides a transparent, secure, and trustworthy model of blockchain where the transactions between the nodes are concerned. DLT has emerged to automate business processes and operations without depending on a centralized third party [1][4]. The smart implementation of blockchain in healthcare is also gaining attention for the achievement of a decentralized system for remote patient monitoring [5], tamper-proof patient-data-storage management [6], and to preserve privacy in the healthcare sector [7]. Practitioners have also implemented the concepts of blockchain in various domains to omit the centralized systems by using distributed systems, such as in trade finance [8], healthcare, electronic voting [9], farming, and the insurance sector [10][11], in order to depict the significance of blockchain.

The vehicular ad hoc network (VANET) is one of the major components of intelligent transportation systems (ITSs). Therefore, the current research always takes care of VANETs in realm of intelligent transportation systems. The smart implementation of VANETs is imperative, and it offers several advantages for different industries. For example, oil marketing companies (OMCs) are eager to have a digitalized system to keep tabs on their fleets and drivers, along with the product movement. Similarly, logistics companies need to have an intelligent transportation system to minimize delays and maximize the performance of deliveries. The smart implementation of VANETs has the potential to take care of the needs of todayâs industries. The further applications of VANETs, with respect to the current era, are supply chain management, solid waste management, autonomous transportation, etc.

VANETs have gained significant importance in research areas since the last decade because of their distinctive characteristics, such as mobility, advance topology, and wireless connected vehicular technology. VANETs are being recognized by both the industry and academia for their implementation on larger scales [12]. In the VANETs, the communication across vehicles and the monitoring office plays a significant role. The objective of the dynamic vehicular network is to precisely circulate the notification of events, such as weather alerts, road blockages, and accidents, as well as emergencies such as roll overs, etc. However, there are limitations of the vehicular network for passing critical messages in the specified radius under a dynamic vehicular environment because of the presence of suspicious vehicles. The security issues of the traditional vehicular network are ultimately exposed. The research related to intelligent transportation systems determines and classifies the attacks and threats related to VANETs by period [13]. The malevolent node can transmit false information by disseminating other important real-time messages. This malicious behavior of nodes can result in the loss of lives and assets. Thus, this is identified as the greatest challenge for the VANET.

2. Blockchain Framework for VANETs

The blockchain-based research methodologies and techniques were determined from the selected articles to answer RQ2. The highlighted blockchain techniques can be employed to improve VANETs. There are 10 techniques that are examined in detail and illustrated in **Figure 1**, and the rest of the techniques are mentioned as âotherâ. **Figure 2** segregates the numbers of studies with regard to the techniques in order to demonstrate the significance of the studies against the techniques.

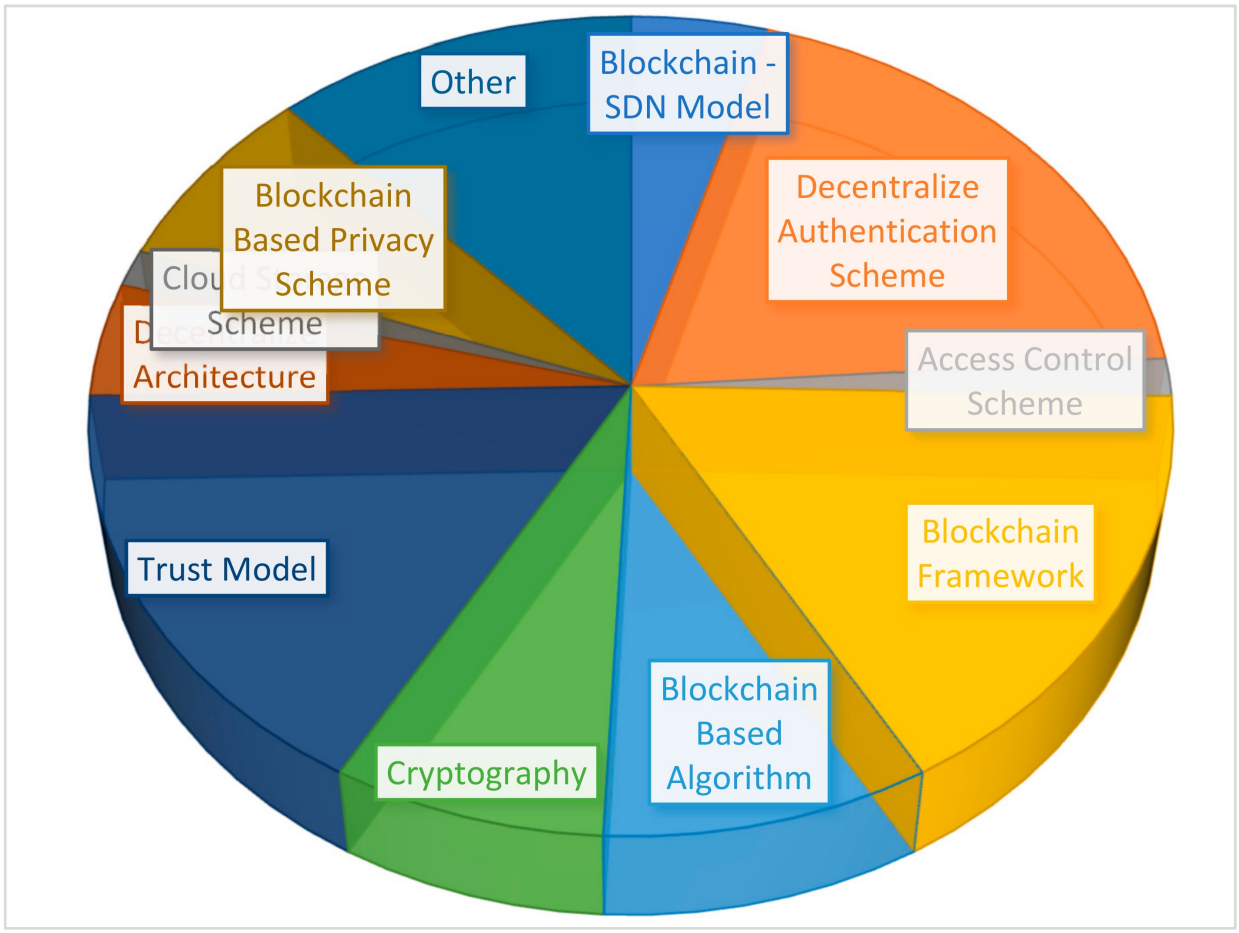

Figure 1. An overview and classification of blockchain techniques.

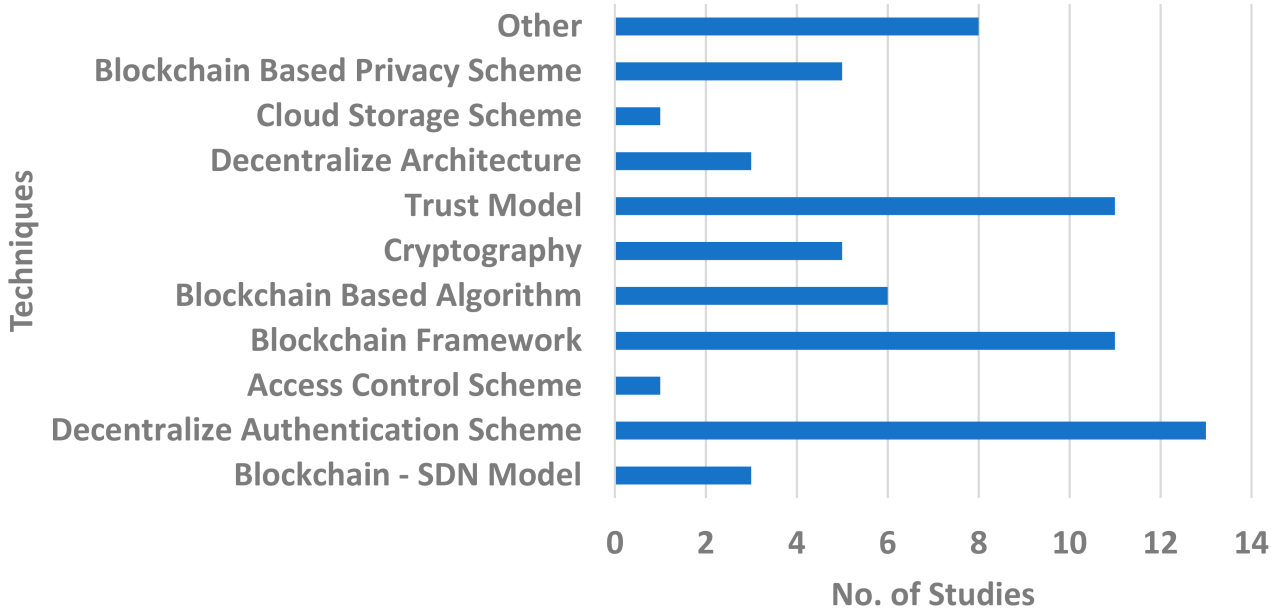

Figure 2. Blockchain techniques and publications.

In **Figure 1**, the blockchain-based techniques are illustrated, and these can be employed to obtain blockchain-enabled VANETs. Blockchain-enabled frameworks [14], decentralized architectures, and techniques based on cryptography are discussed in the majority of the selected studies in relation to overcoming the integration of the blockchain and VANETs.

Figure 2 emphasizes the techniques of blockchain and their significance can be analyzed on the basis of the numbers of studies on them. Blockchain frameworks and decentralized authentication schemes are discussed in 24 aggregated studies out of 68, which shows that blockchain

frameworks are being employed in different IoT sectors. Connected vehicles (CVs) are one of the most promising areas of research in the realm of blockchain. Therefore, the framework for blockchain and CVs is also studied in the most recent research in order to understand the dynamics [15].

3. Decentralized Architecture for VANETs

As can be seen in **Figure 2**, the blockchain framework and the decentralized authentication mechanism are discussed in a total of 24 studies out of 68 shortlisted articles. Furthermore, the practically possible decentralized architecture is discussed in only 3 studies out of 68. Therefore, an advanced decentralized architecture is one of the most prominent needs of time. The state of the architecture is demonstrated in **Figure 3**.

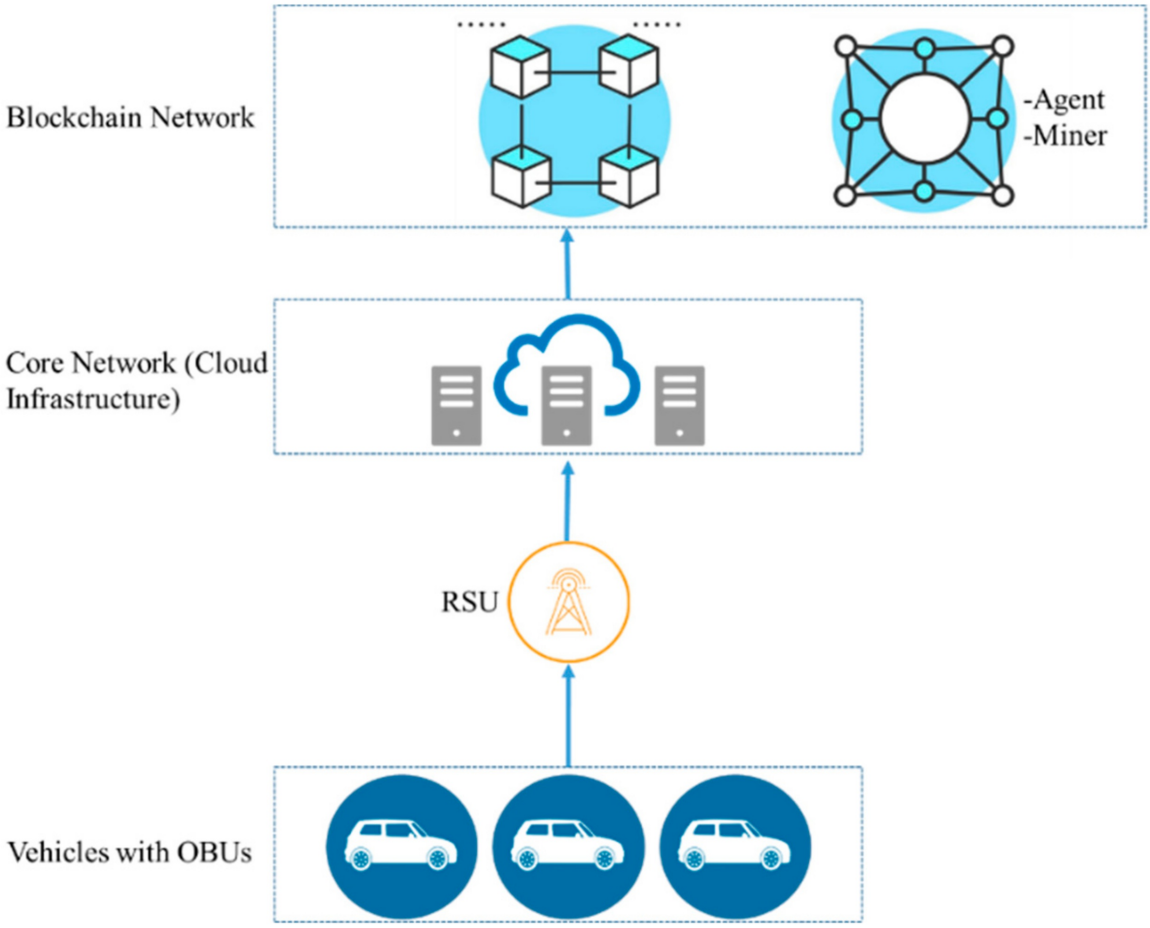

Figure 3. Decentralized architecture for VANETs.

The identity and privacy of vehicles and their locations were analyzed using the construction approach of the IoT chain architecture and private blockchain [5][16] to obtain a blockchain-based architecture for VANETs, as is shown in **Figure 13**. The rectified and analyzed architecture is based on eight different components: vehicles, the roadside unit (RSU), the onboard unit (OBU), the infrastructure, the blockchain network, the smart contract, the miner, and the agent node.

3.1. Vehicles

Vehicles are considered to be one of the essential moving components of blockchain-enabled VANETs. The onboard units installed in vehicles help facilitate communication with the core network.

3.2. On-Board Unit

The OBU is also known as a tracking device, or a data terminal, which is mounted on the vehicle. This component is responsible for the vehicle communication with servers or adjacent nodes.

3.3. Roadside Unit

The RSU is considered to be an access point in the network. This unit is responsible for collecting data from the OBUs and transmitting it to the core network in real time. The RSU also transmits traffic, emergency, and weather-related information for the assistance of drivers and fleet staff.

3.4. Core Network

The core network consists of several servers and ensures connectivity with vehicles for the data transmission through the RSU. The CA, database, application, and web servers lie in the core network. All the data stored on these servers is encrypted in order to confirm the data integrity and security. The core network is responsible for maintaining all the communication messages in real time for further decision making.

3.5. Blockchain Network

The private chain architecture was examined, in which all the hash values are stored in the network to avoid malicious attacks. However, the data cannot be tampered with or changed because the blockchain is immutable.

3.6. Smart Contracts

The protocols (referred to as âcontractsâ) are clearly defined for the authentication, anonymity, data encoding and decoding, etc. The use of contracts also helps to save transaction costs.

3.7. Agent Node

The participant is considered to be an agent node in a decentralized network. The participants participate in a consensus mechanism and ensure the backup of the network. The agent node also provides correctness across transactions.

3.8. Miner

The special agent node is considered to be a miner node when it tries to solve the mathematical problem and solves it successfully. The miner node solves the puzzle and obtains the legal right to keep the block. The miner node is also responsible for the mining and validating of new blocks. The updated data is saved in a newly established block, and all of the other participants update the respective storage accordingly in the blockchain.

The components of the blockchain-based framework for VANETs are discussed above, and their interactions are demonstrated in **Figure 4**.

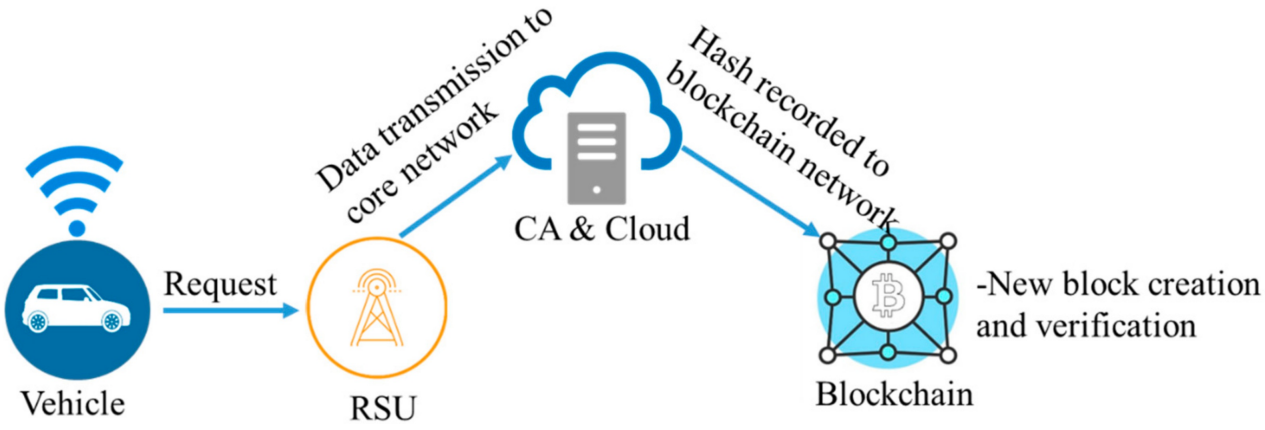

Figure 4. Blockchain-enabled VANET communication architecture.

4. Blockchain and the IoT/VANET Challenges, Limitations, and Techniques

To answer RQ3, **Table 1** explains the methods, challenges and limitations when blockchain integration takes place with VANETs. The advantages and challenges of the traditional models are described as follows: The Bayesian inference model [17] provides the mechanism for decentralized trust management and ensures the consistency and reliability of the storage or database. The composition of the trust management and privacy preservation is one of the major drawbacks of this methodology. The proof of work (POW) is used as a consensus mechanism to validate the authentic and deserving nodes that have good reputations and computing power. In proposed architecture, the message exchange and identification of malicious nodes can be managed by using POW. The provision of information sharing will only be available across vehicles or entities having the capability to prove their worth by solving a puzzle. The POW [18] needs further enhancement to deal with the crucial event message dissemination in dynamic topology in order to achieve low computation and maximum throughput. The proof of driving mechanism is also highlighted by practitioners to mitigate the issues of the POW and proof of stake. The conditional anonymity and improved transparency are observed in the blockchain-based anonymous reputation system (BARS) [19], but it is also vulnerable to various attacks. The certificate less public key signature (CL-PKS) [20] is recognized as one of the efficient methods for vehicle-to-infrastructure communication with lower computation costs. However, it needs to be enhanced more for vehicle-to-vehicle communication. The hierarchical temporal memory (HTM) method [21] was found to be effective and efficient for identifying malicious users, but the challenge of battling frequent attacks persists for this methodology. Similarly, the implementation of an improved growing hierarchical self-organizing map (I-GHSOM) is critically important to achieving intrusion detection functionality. It can be used in the proposed decentralized architecture as a composite mechanism to handle the large number of vehicles in dynamic topology, and to intercept intrusions accordingly for faster and more secure message transmission. The I-GHSOM [22] is quick compared to other methods for detecting multiple types of attacks. The message-by-vehicle can be mined quickly by using this method. However, it needs to be improved in terms of the management of the overheads. The better effectiveness and enhanced data transmission were analyzed under the methodology of unified trust management, but this lacks security because of virtualization and software-defined networks [23] Lastly, the methodology of blockchain-based VANETs [9] was analyzed and was recognized as having one of the most effective data processing times, as well as privacy protection. Earlier, this methodology depended on trusted centralized entities, but the advancement of blockchain has made it decentralized and distributed. However, this methodology is regarded as the most useful for when blockchain meets VANETs.

Table 1. Methods/techniques lead to blockchain-enabled VANETs.

Article	Year	Method	Advantages	Drawbacks
[24] (Li et al., 2019)	2019	Blockchain Based VANETs	This is the most advanced methodology used for state of the art privacy protection and real time data transmission across vehicle to everything	In nascent stages, this methodology relied on trusted centralized entities with a drawback of center point failure, but the advancement of blockchain has made it decentralized and distributed in all as aspects. However, this methodology is regarded as the most useful when blockchain meets VANETs.
[17] (Xia et al., 2020)	2020	Bayesian Model	This method provides mechanism for decentralize trust management and ensures consistency and reliability of the storage or database	The composition of trust management and privacy preservation is one of the major drawbacks of this methodology.
[18] (Kudva et al., 2021)	2020	Proof of Work	This method provides trustworthiness without storage overheads	It needs enhancement to deal with crucial event message dissemination for better performance.
[19] (She et al., 2019)	2019	BARS	This method provides transparency and anonymity and also ensure effective and robust mechanism	This methodology is more vulnerable to various attacks.
[20] (Ali et al., 2019)	2019	CL-PKS	This method provides reliable communication between vehicles to infrastructure with less computational cost.	This method lacks in vehicle-to-vehicle communication.
[21] (Hasrouny et al., 2019)	2019	HTM	This method provides trustworthiness with quick and effective identification of malicious users	This method cannot handle frequent attacks which makes it more vulnerable against the frequent attacks.
[22] (Liang et al., 2019)	2019	I-GHSOM	This method has the ability to detect the attacks rapidly. It also ensure quick encoding of real time messages transmitted by vehicles.	This method needs to improve in terms of management of overheads.
[23] (He et al., 2019)	2019	Unified Trust Management	This method provides effective data transmission and trust management mechanism	This method lacks in security due to virtualization and security of software-defined networks.

Table 1 defines the methodologies and highlights the challenges for VANETs, which are addressed by employing the inherent characteristics of blockchain technology. The detailed list of the blockchain issues is presented in **Figure 4**, and these are addressed by integrating the blockchain with IoT technologies. **Figure 5** highlights that 14 out of 68 studies discuss the issues of trust management and its resolutions. Privacy management is discussed in 13 out of 68 studies, with general security issues discussed in 16 selected studies, which makes it still one of the most prominent issues in blockchain-based VANETs. Issues regarding the proposed frameworks of blockchain are discussed in three of the selected studies and were validated accordingly.

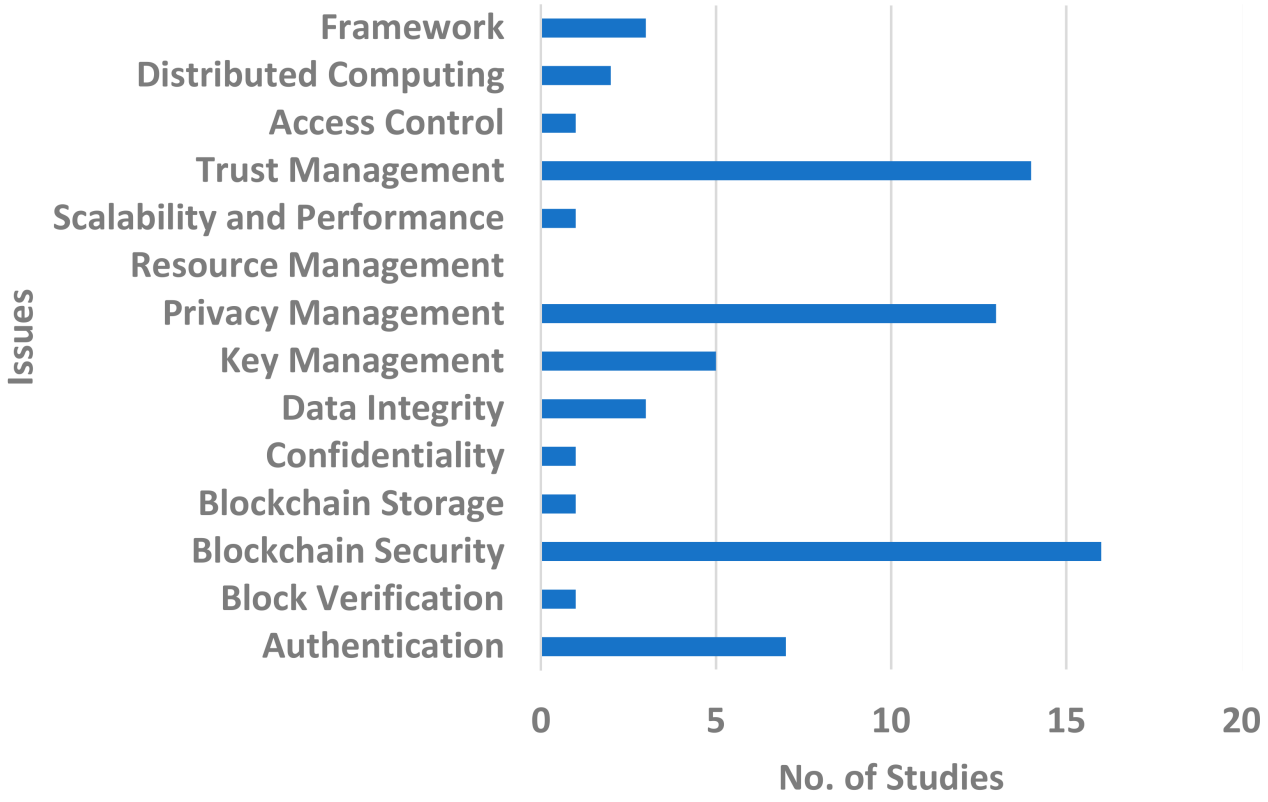

Figure 5. General blockchain issues and numbers of studies.

Lastly, distributed and fog computing are also hot areas for practitioners since the blockchain conference took place in 2018 for future research and directions.

References

1. Cole, R.; Stevenson, M.; Aitken, J. Blockchain technology: Implications for operations and supply chain management. Supply Chain. Manag. Int. J. 2019, 24, 469â483.
2. TÃ¶nnissen, S.; Teuteberg, F. Analysing the impact of blockchain-technology for operations and supply chain management: An explanatory model drawn from multiple case studies. Int. J. Inf. Manag. 2020, 52, 101953.
3. Ãlvares, P.; Silva, L.; Magaia, N. Blockchain-Based Solutions for UAV-Assisted Connected Vehicle Networks in Smart Cities: A Review, Open Issues, and Future Perspectives. Telecom 2021, 2, 108â140.
4. Alladi, T.; Chamola, V.; Parizi, R.M.; Choo, K.-K.R. Blockchain Applications for Industry 4.0 and Industrial IoT: A Review. IEEE Access 2019, 7, 176935â176951.
5. Dwivedi, A.D.; Srivastava, G.; Dhar, S.; Singh, R. A Decentralized Privacy-Preserving Healthcare

Blockchain for IoT. Sensors 2019, 19, 326.

6. Mani, V.; Manickam, P.; Alotaibi, Y.; Alghamdi, S.; Khalaf, O.I. Hyperledger Healthchain: Patient-Centric IPFS-Based Storage of Health Records. Electronics 2021, 10, 3003.
7. Azaria, A.; Ekblaw, A.; Vieira, T.; Lippman, A. MedRec: Using Blockchain for Medical Data Access and Permission Management. In Proceedings of the 2016 2nd International Conference on Open and Big Data (OBD), Vienna, Austria, 22â24 August 2016; pp. 25â30.
8. Treleaven, P.; Brown, R.G.; Yang, D. Blockchain Technology in Finance. Computer 2017, 50, 14â17.
9. Pawlak, M.; Poniszewska-MaraÅda, A.; Kryvinska, N. Towards the intelligent agents for blockchain e-voting system. Procedia Comput. Sci. 2018, 141, 239â246.
10. Sheth, A.; Subramanian, H. Blockchain and contract theory: Modeling smart contracts using insurance markets. Manag. Financ. 2019, 46, 803â814.
11. Jha, N.; Prashar, D.; Khalaf, O.I.; Alotaibi, Y.; Alsufyani, A.; Alghamdi, S. Blockchain Based Crop Insurance: A Decentralized Insurance System for Modernization of Indian Farmers. Sustainability 2021, 13, 8921.
12. Syed, T.A.; Alzahrani, A.; Jan, S.; Siddiqui, M.S.; Nadeem, A.; Alghamdi, T. A Comparative Analysis of Blockchain Architecture and its Applications: Problems and Recommendations. IEEE Access 2019, 7, 176838â176869.
13. Wan, P.K.; Huang, L.; Holtskog, H. Blockchain-Enabled Information Sharing within a Supply Chain: A Systematic Literature Review. IEEE Access 2020, 8, 49645â49656.
14. Bonadio, A.; Chiti, F.; Fantacci, R.; Vespri, V. An integrated framework for blockchain inspired fog communications and computing in Internet of Vehicles. J. Ambient Intell. Humaniz. Comput. 2019, 11, 755â762.
15. Xu, X.; Zeng, Z.; Yang, S.; Shao, H. A Novel Blockchain Framework for Industrial IoT Edge Computing. Sensors 2020, 20, 2061.
16. Vaidya, B.; Mouftah, H.T. IoT Applications and Services for Connected and Autonomous Electric Vehicles. Arab. J. Sci. Eng. 2020, 45, 2559â2569.
17. Xia, S.; Lin, F.; Chen, Z.; Tang, C.; Ma, Y.; Yu, X. A Bayesian Game Based Vehicle-to-Vehicle Electricity Trading Scheme for Blockchain-Enabled Internet of Vehicles. IEEE Trans. Veh. Technol. 2020, 69, 6856â6868.
18. Kudva, S.; Badsha, S.; Sengupta, S.; Khalil, I.; Zomaya, A. Towards secure and practical consensus for blockchain based VANET. Inf. Sci. 2021, 545, 170â187.
19. She, W.; Liu, Q.; Tian, Z.; Chen, J.-S.; Wang, B.; Liu, W. Blockchain Trust Model for Malicious Node Detection in Wireless Sensor Networks. IEEE Access 2019, 7, 38947â38956.
20. Ali, I.; Gervais, M.; Ahene, E.; Li, F. A blockchain-based certificateless public key signature scheme for vehicle-to-infrastructure communication in VANETs. J. Syst. Archit. 2019, 99, 101636.
21. Hasrouny, H.; Samhat, A.E.; Bassil, C.; Laouiti, A. Trust model for secure group leader-based communications in VANET. Wirel. Netw. 2019, 25, 4639â4661.
22. Liang, J.; Chen, J.; Zhu, Y.; Yu, R. A novel Intrusion Detection System for Vehicular Ad Hoc Networks (VANETs) based on differences of traffic flow and position. Appl. Soft Comput. 2019, 75, 712â727.
23. He, Y.; Yu, F.R.; Wei, Z.; Leung, V. Trust management for secure cognitive radio vehicular ad hoc networks. Ad Hoc Netw. 2019, 86, 154â165.
24. Li, H.; Pei, L.; Liao, D.; Sun, G.; Xu, D. Blockchain Meets VANET: An Architecture for Identity and Location Privacy Protection in VANET. Peer-to-Peer Netw. Appl. 2019, 12, 1178â1193.