IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received December 5, 2021, accepted February 3, 2022, date of publication February 7, 2022, date of current version March 1, 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3149958

Blockchain Technology for Intelligent Transportation Systems: A Systematic Literature Review

RATEB JABBAR[1,2], EYA DHIB[3], AHMED BEN SAID[4], MOEZ KRICHEN[5], (Member, IEEE), NOORA FETAIS[4], (Senior Member, IEEE), ESMAT ZAIDAN[1], AND KAMEL BARKAOUI[2]

[1]Department of International Affairs, College of Arts and Science, Qatar University, Doha, Qatar
[2]Cedric Laboratory, Computer Science Department, Conservatoire National des Arts et Métiers, 75141 Paris, France
[3]Mediatron Laboratory, Higher School of Communication of Tunis, Tunis 2083, Tunisia
[4]College of Engineering, Qatar University, Doha, Qatar
[5]ReDCAD Laboratory, National School of Engineers of Sfax, University of Sfax, Sfax 3029, Tunisia

Corresponding author: Rateb Jabbar (rateb.jabbar@qu.edu.qa)

This work was supported by the Qatar National Research Fund (a member of the Qatar Foundation) through the National Priorities Research Program (NPRP) under Grant NPRP11S-1228-170142.

ABSTRACT The use of Blockchain technology has recently become widespread. It has emerged as an essential tool in various academic and industrial fields, such as healthcare, transportation, finance, cybersecurity, and supply chain management. It is regarded as a decentralized, trustworthy, secure, transparent, and immutable solution that innovates data sharing and management. This survey aims to provide a systematic review of Blockchain application to intelligent transportation systems in general and the Internet of Vehicles (IoV) in particular. The survey is divided into four main parts. First, the Blockchain technology including its opportunities, relative taxonomies, and applications is introduced; basic cryptography is also discussed. Next, the evolution of Blockchain is presented, starting from the primary phase of pre-Bitcoin (fundamentally characterized by classic cryptography systems), followed by the Blockchain 1.0 phase, (characterized by Bitcoin implementation and common consensus protocols), and finally, the Blockchain 2.0 phase (characterized by the implementation of smart contracts, Ethereum, and Hyperledger). We compared and identified the strengths and limitations of each of these implementations. Then, the state of the art of Blockchain-based IoV solutions (BIoV) is explored by referring to a large and trusted source database from the Scopus data bank. For a well-structured and clear discussion, the reviewed literature is classified according to the research direction and implemented IoV layer. Useful tables, statistics, and analysis are also presented. Finally, the open problems and future directions in BIoV research are summarized.

INDEX TERMS Blockchain, automotive communication, internet of vehicles, intelligent transport system, Bitcoin, Ethereum, smart contract, Internet of Things, security.

I. INTRODUCTION

With the rapid increase in number of vehicles over the last two decades, and in spite of notable improvements in infrastructure, the transportation solutions that have been previously formulated and implemented have become insufficient to handle today's ever-increasing traffic problems. The necessity of integrating intelligent transportation systems (ITS) has become more critical. In particular, the purpose of ITS is to reduce traffic problems, enhance traffic efficiency, and contribute to the development of smart roads. Users receive valuable information regarding seat availability and other traffic conditions. Accordingly, safety and comfort are improved, and commuting time is reduced. Owing to rapid developments in innovative computation and communication technologies, the original concept of vehicular ad-hoc networks (VANETs) was transformed into an innovative concept termed as the Internet of Vehicles (IoV) [1]–[3]. The IoV is a necessary prerequisite of the ITS because it enables the interconnection of smart vehicles on the Internet. According to the US Department of Transport (DOT) [4], the IoV can particularly contribute to the reduction in crashes

The associate editor coordinating the review of this manuscript and approving it for publication was Hassan Omar.

involving unimpaired drivers. With the integration of IoV, 79% of such crashes are estimated to be avoidable owing to the effective communication and collaboration among vehicles. The interconnection includes communication with bicycles, pedestrians, and roadside infrastructures. By exchanging messages regarding traffic conditions and information on safety and accidents, global traffic control can reduce environmental pollution, accident rates, and traffic jams [5], [6] while enhancing convenience, comfort, and safety. Consequently, public transportation and pedestrian traffic can be considerably significantly improved. A rapid increase in the integration of ITS is expected in the succeeding years through initiatives, such as ERTICO-ITS Europe [7] and CityVerve Manchester [8], that can contribute to the development of smart cities. The IoV ensures the interconnection between smart vehicles, roadside infrastructures, and pedestrians to respond to the complex functional requirements of the ITS and enables the vehicle-to-everything (V2X) paradigm. However, an increasing number of smart vehicles and related vehicular applications as well as services are expected to inevitably generate enormous amounts of data and considerable network traffic. Moreover, the complex IoV characteristics and context, low latency, and high mobility can result in problems related to security, management, and cloud-based storage. Consequently, ensuring the compatibility and interoperability of IoV entities using different service providers is necessary. Therefore, ensuring that the storage and data exchange of the IoV platform are secure, scalable, flexible, interoperable, distributed, and decentralized is paramount. This further ensures the development of the IoV and the realization of the full potentials of the ITS.

Blockchain technology [9] has fundamentally transformed digital currencies since the introduction of Bitcoin [10]. This new decentralized technology represents a distributed ledger that can maintain an immutable log of transactions occurring within a network. Although the primary research focus is on the use of Blockchain in the financial sector, recently, the scientific communities have shifted their attention to the Internet of Things (IoT) [11] and adopted it to generate a decentralized, trustworthy, and secure environment. The development of Blockchain has led to the emergence of high technology in sensitive and active sectors by ensuring the reliability of information via consensus, immutability of records, and transaction transparency. However, the significant added value of Blockchain is enhanced security and trust. In addition, owing to smart contracts, the optimization and automatization of the handling process of information and cost saving have been achieved. Compared with traditional centralized architectures, Blockchain technology has numerous advantages. However, problems, such as storage limitation, inflexibility, and high costs, must be considered. The combination of Blockchain technology with IoV introduces considerable benefits and opportunities. More specifically, this integration can considerably improve security, intelligence, big data storage, and efficient management of the IoV.

A. RELATED WORKS AND CONTRIBUTIONS OF THIS SURVEY

The studies relevant to Blockchain applications in the transportation industry and their contributions, challenges, and opportunities are summarized in Table 2. Smetanin *et al.* [12] investigated the relevant academic and industrial barriers to Blockchain application in transport management, logistics, and supply chain by focusing on four clusters: traceability/transparency, trade, trust, and technology. However, their study did not analyze the implementation of Blockchain through Hyperledger, Ethereum, and Bitcoin. In fact, the study focused on the application domain, but open problems were not considered. Butt *et al.* [13] explored the privacy issues and critical factors in social IoV (SIoV) environments. The authors explored the factors essential for the privacy of SIoV systems. These factors include security, applications, goals, communication technologies, social relationships, user preferences, context awareness, and architecture. Note that this work only considered the privacy perspective of Blockchain; no other challenges were discussed. Astarita *et al.* [14] used the multi-step methodology to review relevant studies on Blockchain application and identified primary gaps in the literature, current research trends, and possible future challenges. However, topics related to general business, trade, IoT, and trust issues have not been considered. Gupta *et al.* [15] investigated the classification of threats (e.g., wormhole attacks, timing, denial of service (DoS), and impersonation) on autonomous vehicles (AVs) via service availability, accountability, and authentication. A critical merit of this study is that it also includes the taxonomy of AV attacks. However, the authors did not discuss in depth the research challenges related to Blockchain-based AV systems.

El-Switi and Qatawneh [16] investigated the use of Blockchain technology in the market of used vehicles with the aim of eliminating fraud using a secure ledger to log the life-cycle events of vehicles. Because the market of used vehicles is a critical economic sector characterized by numerous stakeholders and high potential for frauds (e.g., odometer frauds), the authors argued that devising a solution for tracking and logging vehicle data is necessary. Most importantly, this study determined the incentives for stakeholders to maintain and manage the Blockchain; critical privacy issues were also emphasized, but the Blockchain limitations were not analyzed. Iqbal *et al.* [17] summarized the recent studies that used Blockchain technology. Although they presented an extensive comparative study of different approaches and scenarios, only 14 research contributions were analyzed and compared. Mendiboure *et al.* [18] analyzed and compared the current applications of Blockchain technology to improve the trust, privacy, and security in vehicular environments. More importantly, they investigated the primary challenges of integrating the Blockchain technology to vehicular networks (e.g., vehicular networks constraints and performance evaluation). However, although the authors extensively focused on the challenges, they did not

consider the application of Blockchain to vehicular networks. Mollah *et al.* [19] surveyed the cutting-edge developments in Blockchain for IoV aimed at identifying potential application areas. However, although the primary problems related to the application of Blockchain to the IoV were analyzed, the classification methodology of analyzed works was not considered. Wang *et al.* [20] surveyed Blockchain-based cybersecurity for vehicular networks and discussed the cybersecurity threat analysis of vehicular networks; however, recent advances in fifth-generation (5G) technology, big data analytics, and machine learning were not considered. Dibaei *et al.* [21] investigated the integration of innovative technologies (e.g., machine learning and Blockchain) to IoV for securing vehicular networks. However, the challenges that hinder the implementation of deep learning and Blockchain in vehicular networks have not been well investigated. Wang *et al.* [20] investigated several aspects (e.g., preserving privacy in IoV, certificate management, trust management, and Blockchain-based IoV security) of the Blockchain implementation in the IoV; however, they did discuss the open issues in detail, and recommendations for further research were not provided. Mikavica and Kostić-Ljubisavljević [22] reviewed state-of-the-art Blockchain architectures according to their primary features and objectives related to security, privacy preservation, and trust management. Their study aimed to enhance security services in vehicular networks. However, they did not focus on the challenges involved in Blockchain implementation; hence, potential directions to resolve such problems were not proposed. Megha *et al.* [23] opted for a software engineering approach to categorize and assess the solutions to problems in the AV industry using Blockchain. The study focused on the ''Applications of Blockchains in the IoVs'' highlighted several aspects of Blockchain implementation in IoVs, and resolved the problems involved. However, the work only considered 22 studies. Khoshavi *et al.* [24] investigated the potential applications of Blockchain in transportation systems and its potential integration to connected and autonomous vehicles (CAVs). More specifically, they compared the maintenance, energy, and security features in terms of Blockchain type, drawbacks, and advantages. Nevertheless, the study did not discuss open issues in detail, and recommendations for further research were not provided. Kumar *et al.* [25] surveyed current studies whose objective is to secure the IoV using Blockchain techniques, such as trust-based, authentication, data sharing, decentralized, distributed, reputation, privacy, and security approaches. An important merit of this study is that it considered the performance evaluation metric tools used by researchers and the timeline from the experimentation perspective. Nevertheless, the study did not discuss open issues in detail, and recommendations for further research were are not provided. Queiroz *et al.* [26] analyzed well-known solutions for Blockchain-based vehicular edge computing (VEC), introduced primary features, limitations, and advantages, and categorized them based on usage scenarios. Moreover, they provided a comprehensive taxonomy of Blockchain and edge computing for the IoV; however, only 14 studies were reviewed.

Previous research works explored the adoption of Blockchain in IoV, provided taxonomies, and highlighted their main features, advantages, and limitations. However, the aforementioned studies have several limitations. First, their extents are limited in terms of the number of reviewed research works. Iqbal *et al.* [17] analyzed 14 studies, and Megha *et al.* [23] and Queiroz *et al.* [26] considered less than 22 studies. Moreover, the reviews did categorize the surveyed studies. For example, Mollah *et al.* [19] did not include the classification methodology of analyzed works. Furthermore, the reviews tended to focus only on one problem related to the use of Blockchain. For example, Butt *et al.* [13] only examined privacy issues related to SIoV environments; Dibaei *et al.* [21] only focused on security issues and did not investigate in depth the challenges of implementing deep learning and Blockchain in vehicular networks. Some studies, such as [12], [15], [16], [22], [23], [27], did not consider the challenges or limitations of Blockchain. Finally, virtually all studies only focused on the application of Blockchain to IOVs. Hence, in upcoming studies, the investigation of the used Blockchain architectures is recommended. Accordingly, future reviews must systematically and comprehensively analyze the limitations and challenges of the IoV (which is regarded as a crucial enabler of ITS) as well as future research directions and opportunities. In addition to the systematic analysis of research contributions categorized according to use, the classification must consider the IoT architecture. In this work, we reviewed the literature on state-of-the-art Blockchain technology and traced its evolution from the pre-Bitcoin phase (as represented by fundamental cryptographic systems) to the Blockchain 2.0 phase (as represented by the implementation of Hyperledger and Ethereum as well as smart contracts). After highlighting various Blockchain applications across multiple domains, we focused on intelligent transport applications to IoV networks and classified related research into six categories: security, transportation applications, energy, communication and network, data management, and payments. Then, for each direction, we categorized the literature according to their IoV layer affiliation. Finally, we identified the main challenges in this field and proposed future research directions.

B. ARTICLE ORGANISATION

The rest of the paper is structured as follows. Section II presents a global overview of Blockchain technology and its opportunities, challenges, related cryptography fundamentals, relative taxonomies, and different uses. In Section III, we present a detailed chronological evolution of the history of Blockchain, divided into three main phases: pre-Bitcoin, Blockchain 1.0, and Blockchain 2.0. In this section, we also discuss the existing consensus algorithms as well as introduce and compare three popular Blockchain implementations: Bitcoin, Ethereum, and Hyperledger. In Section IV, different

FIGURE 1. Key concepts of Blockchain technology.

IoV-layered architecture models are discussed. Section V reviews how the Blockchain technology is applied to ITS from the IoV perspective. In Section VI, future research opportunities are identified. Finally, in Section VII, the concluding remarks of this paper are presented. Additionally, the list of acronyms is presented in Table 1.

II. OVERVIEW OF BLOCKCHAIN

Blockchain is an innovative technology that forms the basis of the cryptocurrency Bitcoin [10], which was formulated by Satoshi Nakamoto (pseudonym) who proposed it in 2008 and then released it in 2009. However, the original paper did not discuss the Blockchain technology [28]. Therefore, it may be stated that Blockchain is an unintentionally invented technology with potential applications to numerous fields. The main objective of Blockchain is to ensure that transactions of value within a network of entities that cannot be trusted go through a trusted intermediary [29]. The emergence of Blockchain has contributed to the paradigm shift in computer science. The aim of this section is to explain the Blockchain concept as well as its beginnings, development, and relevance to proposed solutions to problems.

A. BLOCKCHAIN DEFINITION

Blockchain [30], [31] represents a database structured as a one-dimensional hash chain of blocks whose origins are in a genesis block. The distribution and maintenance of Blockchain are accomplished by a group of participants of a peer-to-peer network who do not trust each other (Figure 1). Thus, a consensus mechanism must exist among the participants such that they can all agree about the state of the database. The introduction of a data structure to fingerprint the information can enhance the storage efficacy of Blockchain. In particular, digital signatures must be used to ensure that only authorized entities can implement data change.

Blockchain is argued to be a linked list implemented with hash pointers [32]; this simply means that it is a one-dimensional hash chain.

Some scholars, such as Abeyratne and Monfared [34], argue that Blockchain is a database distributed in a peer-to-peer network. Nevertheless, the distributed property is not a requirement for Blockchain; instead, it is an orderly application of the Blockchain database. The Blockchain is powerful due to this property; accordingly, it is typically known as a distributed database. A decentralized distribution means that trust among participants is not necessary to manage Blockchain [35]. The database depends on a chain structure. Consequently, long chains consume considerable amounts of memory. A hash pointer stored in one block points to

TABLE 1. List of acronyms.

Intelligent Transportation Systems	ITS
Internet of Vehicles	IoV
Blockchain based IoV solutions	BIoV
Vehicular Ad hoc network	VANET
US Department of Transport	DOT
Vehicle to Everything	V2X
Social Internet of Vehicle	SIoV
Denial of Service	DoS
Autonomous Vehicle	AV
Internet of Things	IoT
Connected and Autonomous Vehicle	CAV
Vehicular Edge Computing	VEC
Asymmetric Cryptography	AC
Message Digest Algorithm 5	MD5
Secure Hash Algorithm 1	SHA 1
Proof of Work	PoW
Proof of Stake	PoS
Delegated Proof of Stake	DPoS
Practical Byzantine Fault Tolerance	PBFT
Proof of Elapsed Time	PoET
Proof of Activity	PoAc
Proof of Burn	PoB
Proof of Capacity	PoC
Decentralized Software Platform	ĐApps
Ethereum Blockchain as a Service	EBaaS
Ethereum Virtual Machine	EVM
Transactions Per Second	TPS
Web Assembly	WASM
Roadside Unit	RSU
Message Authentication Code	MAC
Electric Vehicles	EVs
Vehicle Data Collection System	VDCS
Authorized Proof of Stakes	APoS
Distributed Denial of Service	DDoS
Smart Contract Security Verification Standard	SCSVS
Proof of Participation and Fees	PoPF
Proof of Search	PoSe
Proof of Accuracy	PoA
Proof of Sincerity	PoSn
Proof of Learning	PoL
Proof of Benefit	ePoB
Proof of Experience	PoEx
Proof of Evaluation	PoE
Proof of Adjourn	PoAj
Federated Learning	FL
Directed Acyclic Graph	DAG
Deep Reinforcement Learning	DRL
Device to Device	D2D
Network Functions Virtualization	NFV
Software Defined Networking	SDN

TABLE 2. Existing surveys in BIoV.

Authors	Year	Survey objectives	Merits	Demerits
Pournader et al. [33]	2020	Discussed relevant academic and industrial barriers to Blockchain application in transport management, logistics, and supply chain.	Investigated relevant academic and industrial barriers to Blockchain application in transport management, logistics, and supply chain by particularly focusing on four clusters: Traceability/Transparency, Trade, Trust, and Technology	Did not analyze Blockchain implementation, such as Hyperledger, Ethereum, and Bitcoin; focus was on the application domain, but open issues were not considered
Butt et al. [13]	2019	Investigated privacy issues and critical factors related to maintaining privacy in SIoV environments	Investigated the challenges related to the privacy of SIoV systems by exploring factors such as security, applications, goals, communication technologies, social relationships, user preferences, context-awareness, and architecture	Only explored privacy issues related to social SIoV environments; no other challenges were discussed
Astarita et al. [14]	2020	Discussed relevant studies regarding the application of Blockchain-based systems in transportation.	Identified primary research gaps in the literature, current research trends, and possible future challenges using multistep technology	Did not analyze documents pertaining to general business, trade, trust issues, and the Internet of Things
Gupta et al. [15]	2020	Comprehensively and systematically reviewed privacy and security issues based on AVs and related countermeasures	Investigated the classification of threats on AVs via service availability, accountability, and authentication; it included the taxonomy of AV attacks	Did not discuss in detail research challenges related to Blockchain-based AV systems
El-Switi et al. [16]	2021	Investigated the status of current research with regard to the use of Blockchain in the market of used vehicles with the aim of eliminating fraud using a secure ledger to log vehicle lifecycle events	Identified incentives for stakeholders to maintain and manage the Blockchain as well as emphasize critical privacy issues	Did not discuss limitations of Blockchain
Iqbal et al. [17]	2021	Summarized the newest studies that used Blockchain technology because of its inherent security features	Summarized some of the latest articles on Blockchain technology due to inherent security features of Blockchain	Only analyzed 14 studies
Mendiboure et al. [18]	2020	Analyzed and compared current applications of Blockchain technology to improve trust, privacy, and security in vehicular environments	Analyzed the primary challenges in the integration of Blockchain technology to vehicular networks (e.g., vehicular networks, constraints, and performance evaluation)	Did not consider the application of Blockchain to vehicular networks
Mollah et al. [19]	2021	Surveyed the cutting-edge developments in Blockchain for IoV	Analyzed main challenges related to the Blockchain application in IoV	Did not include the classification methodology of analyzed works
Wang et al. [20]	2020	Surveyed the recent application of Blockchain for cybersecurity in vehicular technology	Discussed the security application of Blockchain technology and analyzed cybersecurity threats of vehicular networks	Did not include emerging technologies, such as 5G, big data, and the latest developments in machine learning
Dibaei et al. [21]	2021	Investigated innovative technologies (e.g., machine learning) and discussed the use of Blockchain as a cybersecurity defense mechanism in vehicular networks	Analyzed in detail the security vulnerabilities in vehicular networks	Challenges of implementing deep learning and Blockchain in vehicular networks were not well investigated
Wang et al. [27]	2021	Investigated several aspects of Blockchain implementation in IoV (e.g., privacy and security)	Investigated recent works considering seven aspects (e.g., preserving privacy in IoV, certificate management, trust management, and Blockchain-based IoV security)	Did not discuss open issues in detail; recommendations for further research were not provided
Mikavica et al. [22]	2021	Analyzed Blockchain-enabled solutions regarding trust, privacy, and security issues in vehicular networks	Analyzed Blockchain-based solutions aimed at improving security services in vehicular networks	Did not discuss open issues in detail; recommendations for further research were not provided
Megha et al. [23]	2020	Described, categorized, and assessed solutions to problems in the autonomous vehicle industry that employ Blockchain	Employed a software engineering approach to categorize current studies according to promoted quality attributes and resolved challenges	Only considered 21 studies
Khoshavi et al. [24]	2021	Investigated the potential applications of Blockchain in transportation systems and potential integration with CAVs	Compared maintenance, energy, and security methods in terms of Blockchain type, drawbacks, and advantages	Did not discuss open issues in detail; recommendations for further research were not provided
Kumar et al. [25]	2021	Surveyed current studies with the aim of securing the IoV using Blockchain techniques, such as trust-based, authentication, data-sharing, decentralized, distributed, reputation, privacy, and security approaches	Considered the performance evaluation metrics, tools used by researchers, and timeline from the perspective of experimentation	Did not discuss open issues in detail; recommendations for further research were not provided
Queiroz et al. [26]	2020	Analyzed well-known solutions for Blockchain-based VEC, introduced primary features, limitations, and advantages, and categorized them to provide subsidies for further proposals	Provided comprehensive taxonomy of Blockchain and edge computing for IoV	Only considered 14 studies

the previous block. Hence, modifying data in the previous block without invalidating the pointer in the next block is not possible. A Merkle tree [36] can resolve this problem because the participants can be able to keep a valid copy of only the data relevant to them by fingerprinting the transactions using a data structure. This data structure is not necessary for the Blockchain; however, it is a beneficial tool for increasing the storage efficiency for Blockchain participants and improving overall usefulness. The use of digital signatures in Blockchain ensures the authenticity of the origin of issued database transactions; accordingly, data can be linked to the owner. This tool is not a requirement for the Blockchain because a transaction must simply be consistent to be valid. In other words, transactions for altering data must have adequate identification, which can be achieved using digital signatures. With regard to monetary systems, this means that only owners control their money.

B. OPPORTUNITIES AND DISADVANTAGES

Currently, Blockchain technology has a wide application range beyond cryptocurrency. Its decentralized architecture relieves the system from known central authority limits, such as security vulnerabilities and bottleneck access to networks. Historical and current data as well as relative changes are all transparently recorded and publicly viewable to any seeker. Blockchain is also an immutable ledger where data are difficult to alter or tamper with. It ensures a high and secure data sharing channel that can be attributed to the efficient decentralized cryptographic mechanisms it employs. In addition, the data exchange operations and transactions in Blockchain are faster and cost-effective than those in traditional systems; however, big data processing remains a challenge. Regarding Bitcoin, blocks are currently restricted to a size of 1 MB, and at approximately every 10 min, a new block is mined. As a result, the Bitcoin network is limited to seven transactions per second, rendering it incapable of coping with high-frequency trading. However, bigger blocks require more storage space and have a more gradual propagation over the network. This can gradually lead to centralization because users generally prefer to maintain a big Blockchain. The two well-known Blockchain implementations, Bitcoin and Ethereum, have sizes of 351 GB and more than 1 TB, respectively [37], [38]. As a result, balancing block size and security has become difficult.

C. BLOCKCHAIN SYSTEM TYPES

Three primary types of Blockchain systems (private, public, and consortium) are commonly discussed in literature [39]–[43]. The private Blockchain, also called permissioned Blockchain, is a closed and access-restricted system where only pre-verified persons who satisfy certain requirements are allowed to perform certain actions on the Blockchain. Most small-range organizations and business Blockchains favor this Blockchain type; however, it is not suitable for trading scenarios. In contrast, the public Blockchain presents a wide-open permissionless system where anyone can join and have full rights to use it. The auditability and transparency of information are more appreciated because no access limitation is imposed. However, the cost of related mining operations, delay, and synchronization among all participating nodes are high. Public Blockchains are not recommended for long delays or energy-sensitive domains. These two Blockchain types are considerably self-explanatory. The third type, consortium Blockchain, is between the two aforementioned types; it is a semi-private and semi-open Blockchain system where only organizations or participants with the same goals could join the group. It ensures scalability, acceptable delay, and reasonable costs.

D. BLOCKCHAIN KEY CONCEPTS

This section describes the fundamental concepts of cryptography related to key pair encryption, hashing function, and Merkle tree. Further, it defines the Blockchain taxonomy, such as data block and transactions (Figure 2).

1) ASYMMETRIC CRYPTOGRAPHY

Asymmetric cryptography, also known as public key cryptography, is a data encryption–decryption technique that provides an extremely high level of security, information protection, authenticity, and confidentiality. The technique allows a user to sign a transaction in the public register of the Blockchain, therefore certifying that the user is the author. Based on a key pair [43], each user has an appropriate pair of keys (public and private keys). The private key remains private to its user, whereas the public key is accessible to other participants. Let M denote the clearly transferred message and M' be the sent message, as shown in Figure 3. As given by Equation 1, M' is consistently encrypted or signed by the sender's private key:

$$M' = Sign(PrivateKey(PrvS); Message(M)) \quad (1)$$

where PrvS is the private key of sender S.

In turn, the receiver determines the public key that decrypts the message; then, the sender identity is disclosed [44]. Equation 2 illustrates the decryption or verification phase:

$$M = Verify(PublicKey(PrvS); Message(M')) \quad (2)$$

According to the philosophy of asymmetric cryptography, the reliability of the authentication is confirmed because the signature is bound to a signer. Moreover, the provision of non-repudiation is insufficient to allow a sender to deny sending a particular message. Moreover, the message cannot be changed in transit because this implies the invalidation of verification; thus, integrity is ensured. Moreover, a digital signature ensures the validity of the message origin because the sender cannot forge a signature, which is based on previously signed messages [45].

2) CRYPTOGRAPHIC HASH FUNCTION

Figure 4 illustrates the hashing-based cryptography scenario. Hash functions are widely used in asymmetric cryptography

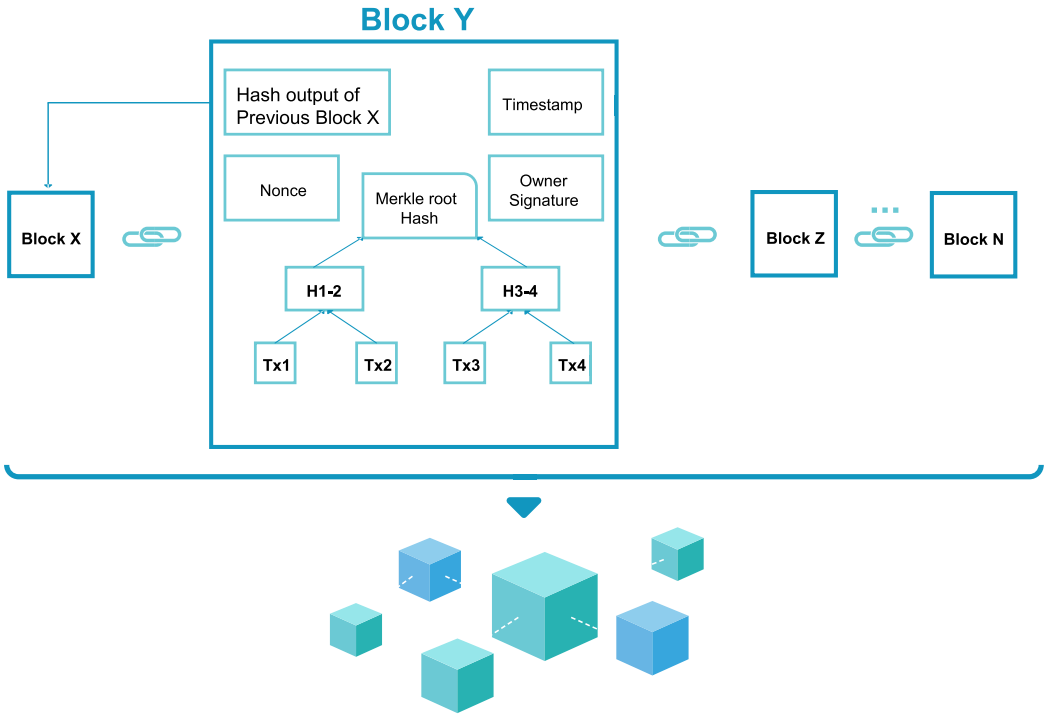
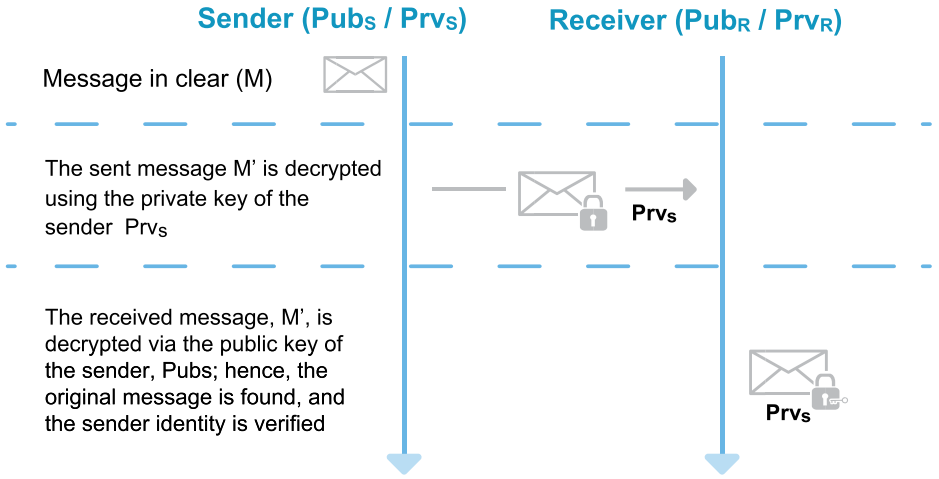


FIGURE 2. Generic chain of blocks.



Prv_S: Private key of the sender S; Pub_S: public key of the sender S,
Prv_R: Private key of the receiver R; Pub_R: public key of the receiver R

FIGURE 3. Asymetric cyptography procedure.

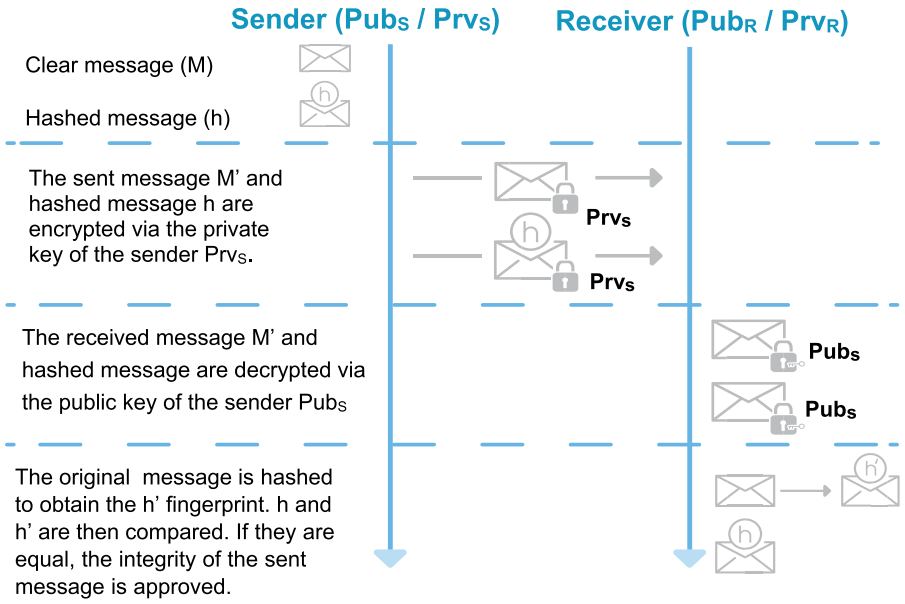
for integrity verification purposes [46]. A cryptographic hash function, H, is an algorithm that accepts a message, M, with a variable input length and outputs a fixed-length digest or fingerprint, h [41]. Equation 3 mathematically formulates the hash function, as follows:

$$h = H(M), M : message \tag{3}$$

The equation is also known as a one-way hash function because recovering the original message, M, from the fingerprint, h, is virtually impossible. Additionally, it is difficult to find two different message inputs, M and N, with an identical hash output (Equation 4). The hash function is collision-free because the occurrence of collisions is extremely rare [47]:

$$H(M) \neq H(N), \quad if\ M \neq N, M, N : messages \tag{4}$$

Some examples of commonly used hash functions are MD5, SHA-1, SHA-3, SHA-256, and SHA-512. The last three are used to ensure the authenticity of the Blockchain.



Prv_S: Private key of sender S; Pub_S: public key of sender S,
Prv_R: Private key of receiver R; Pub_R: public key of receiver R

FIGURE 4. Hashing-based cryptography process.

FIGURE 5. Hash pointer illustration.

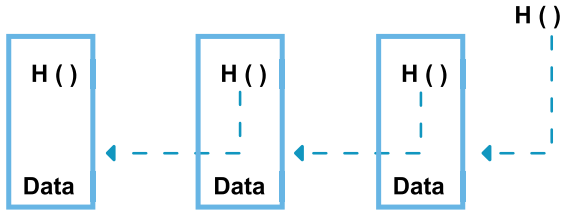


FIGURE 6. Hash chain.

3) HASH POINTER

The hash pointer function, shown in Figure 5, is a cryptographic hash (of certain data) and a storage location pointer. The input can be calculated with the pointer and data, which are guaranteed to be tamper-proof [32]. The integrity property is derived from the cryptographic hash function. Consider two messages, M and N. Their hash digests, H(M) and H(N), are equal if and only if the messages are identical, i.e., M = N. Thus, the content changes with the hash value of a data element.

4) HASH CHAIN

When hash pointers are used to link different data elements, the process is known as a hash chain [41]. A hash pointer represents the head of the chain. A one-dimensional hash chain represents a linked list utilizing a hash pointer derived from a genesis element, as shown in Figure 6. The alteration of one element invalidates all subsequent elements of the chain; hence, a hash pointer update is highly recommended. The hash function is collision-free. Consequently, the value of the hash pointer in the next element and that of the hash of the tampered element cannot be the same. Moreover, if the chain was tampered, it could be detected. In fact, when one element is tampered, all subsequent elements must be changed to preserve the chain consistency. The alteration modifies the head of the chain, compromising the integrity of the entire chain [32].

5) MERKLE TREE

The Merkle tree, also called a hash tree, presents a binary data structure that more securely and efficiently encodes Blockchain data. Instead of hashing a large data block, which is a costly operation in terms of time, it is partitioned into small data elements. In turn, each element is separately hashed. The corresponding hash digests are grouped in pairs, concatenated, and re-hashed until all data elements of the current block are processed. In some cases, a block contains an odd number of data elements; hence, one element is doubled

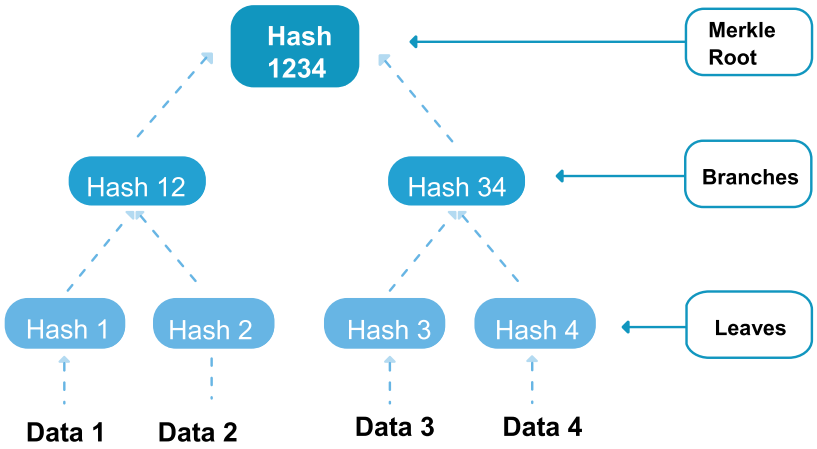


FIGURE 7. Hash Merkle tree.

before hashing is executed. Figure 7 illustrates a highly simplified data block with only four data elements. The bottom layer of the tree represents the hash digest relative to each data element. Hence, ''Hash1'' is the hash print of ''Data1,'' and so on. This layer refers to the leaf nodes of the Merkle Tree. The intermediate hashes form branch nodes, which are the hashes of respective child nodes (leaf or branch nodes); the top hash represents the root. The Merkle proof [48] allows the verification of a leaf value by comparing the public Merkle root and the authentication path information (API) across branch layers. For example, ''Hash 1'' could be authenticated by sending ''Data 1'' (a leaf value) and paths ''Hash 12'' and ''Hash 34''. Thus, the root node computes Hash1' relative to the received value, Data1. Using the sent path, the hash value, Hash12', of the upper branch is calculated by hashing the pair (Hash1', Hash2), and the root value Hash1234' by hashing the pair (Hash12', Hash34). Then, the original Merkle root is compared with the calculated value; data are verified if the values are equal.

6) TRANSACTION

Because Blockchain is a large database, a transaction is the operator that modifies its state. The transaction forms an independent unit of work that verifies four main properties commonly referred to by the acronym ''ACID'' [49]:

- ''Atomicity propriety'' means that a transaction is either fully performed or not at all;
- ''Consistency'' refers to the satisfaction of database constraints after transaction;
- ''Isolation'' ensures that each transaction is independently executed;
- ''Duration'' highlights the sustainability of the transaction effect once completed.

7) BLOCK

A block is defined as a unit encompassing a batch of transactions. Blocks can be similarly chained as elements of a hash chain (Blockchain). A chain of transactions results in an extremely long chain; therefore, building the blocks of units of the hash chain is more efficient. All transactions must be shared with all interested actors. Hence, publishing one transaction at once is inefficient; instead, a block of several transactions must be announced [50]. The block is divided into block header and payload. The block header includes the metadata: timestamp, Merkle root derived from the payload, and hash pointer to the previous block [51]. The payload includes the actual transaction data.

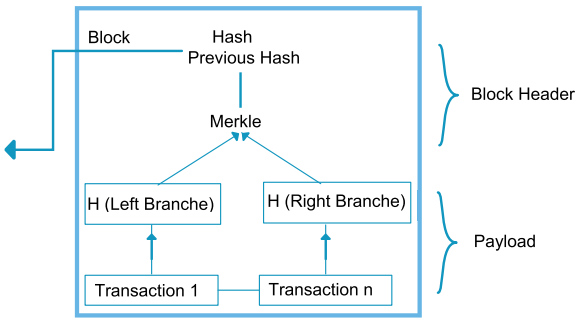


FIGURE 8. Block.

As illustrated in Figure 8, It is created under the Merkle tree, and the block integrates the hash chain units. However, the storage of all actual data does not improve the efficacy or maintain the integrity level of the chain. Therefore, the hash of a block only represents the block header hash [52]. When the transaction is tampered with, the meaning of the Merkle root changes. The block hash also changes when the chain integrity is violated.

8) PEER-TO-PEER NETWORK

A peer-to-peer network represents a collection of loosely combined interacting autonomous nodes. Due to its decentralization, the nodes can join and leave the network unimpeded. In a pure peer-to-peer network, all participating nodes have the same privileges [53]; typically, nodes share resources. A seed node in Blockchain is a known node capable of joining the network [49], [54].

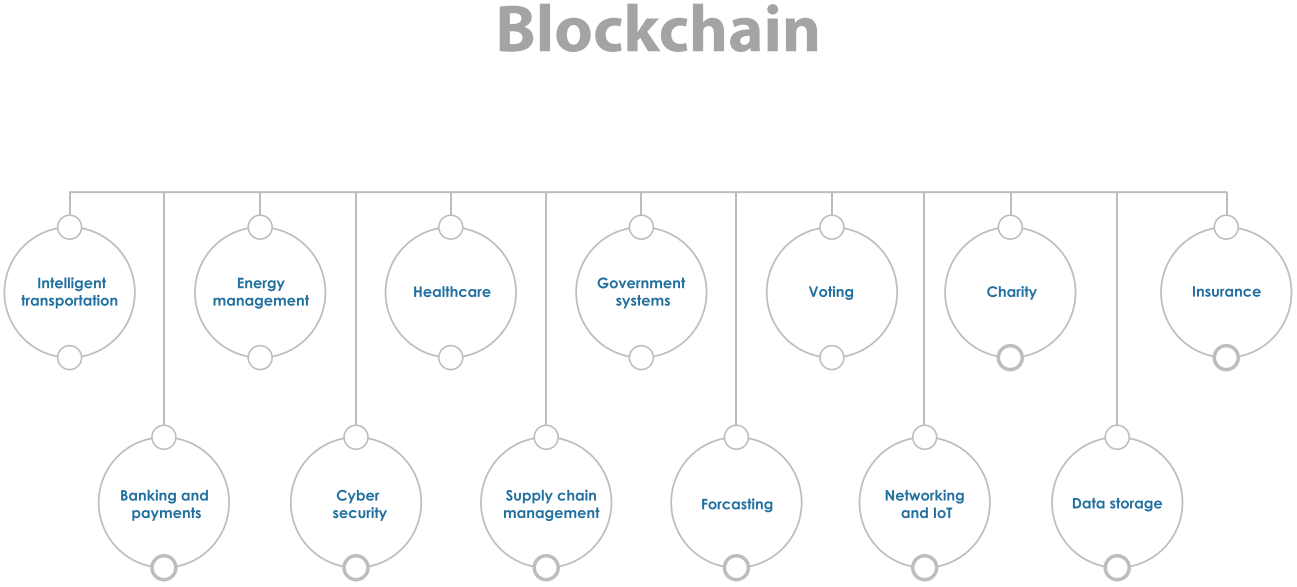


FIGURE 9. Blockchain applications in different domains.

E. BLOCKCHAIN USE CASES

The Blockchain technology has been integrated into many industries and may be incorporated with many others in the next decades (Figure 9). Some examples of these applications are briefly introduced, as follows.

- The banking and payments sector [55]–[60] provide access to financial services that can include countries without traditional banking systems. Payment and other financial operations are facilitated, more efficient, and secure.
- The cybersecurity sector [61]–[63] supports in verifying and securing data using advanced cryptography. The data are less prone to hacking or alteration without authorization. Different from typical traditional legacy systems, an authorized third party or a middleman becomes unnecessary.
- The supply chain management sector [64]–[66] aids in documenting transactions in a permanent decentralized record and monitoring them in a secure and transparent manner. This reduces delays and precludes the further introduction of human errors. Blockchain is also employed to reduce costs, labor, etc. in the supply chain and verify the authenticity or fair trade status of products.
- Forecasting [67] provides a decentralized market for consulting, analysis, and forecasting operations in various domains, such as elections, sports, stock markets, and energy consumption.
- Networking and IoT markets [68], [69] propose the decentralized networks of IoT devices using Blockchain. Because the Blockchain operation is similar to a public ledger for numerous devices, the necessity of a central entity to handle all IoT communication devices is eliminated.
- The global insurance market [70], [71] is based on trust management. Because Blockchain presents a new way of managing trust, it can be applied to verify various types of data in insurance contracts, such as the identity of the insured person.
- Online data storage using Blockchain [72], [73] allows cloud storage to be more secure and robust against attacks, hacking, data loss or human errors.
- Charitable organizations that use Blockchain [74] can be more certain that financial aids and donations reach those who deserve it; Blockchain technology can aid in overcoming inefficiency and corruption.
- Voting [75], [76] presents an area where Blockchain has the greatest potential. It can be used for voter registration, identity verification, and electronic vote counting, ensuring that votes have not been altered, and only legitimate votes are counted. It can potentially reduce organizational expenses significantly while improving voter turnout. It eliminates the necessity of filling printed ballots or visiting polling locations, and people may vote from any location with an Internet connection.
- Government systems [77], [78] are typically slow, opaque, and prone to corruption. Blockchain can reduce bureaucracy and increase the security, transparency, and efficiency of governmental operations.
- Healthcare [79]–[83] is another industry that relies on legacy systems. Hospitals require a secure platform to store and share sensitive data to avoid hacking and privacy breach problems. Blockchain can contribute to the safe storage and sharing of medical records with authorized users. It can aid in improving data security, accuracy, and high-speed diagnostics.
- Energy management [84], [85] used to be a highly centralized industry [86]–[88]. Energy producers and

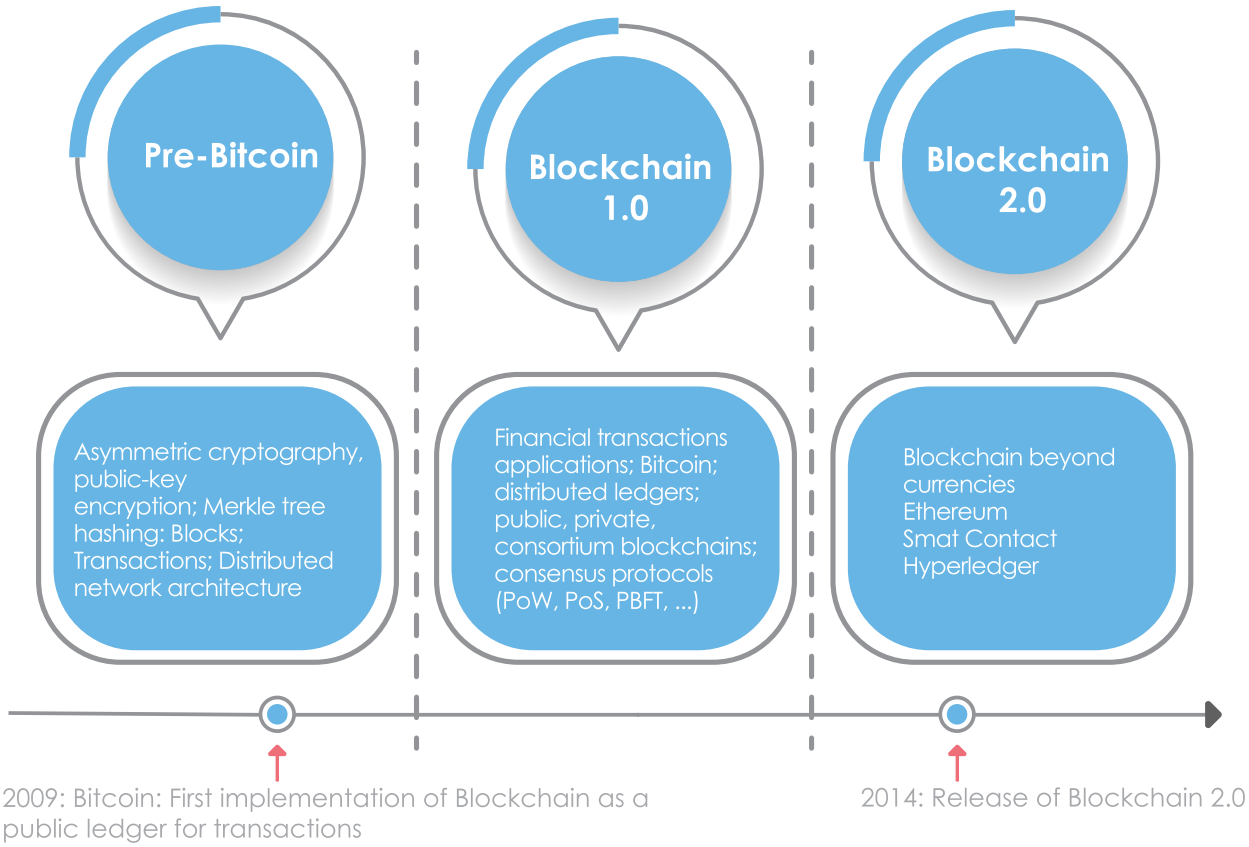


FIGURE 10. History of Blockchain technology.

consumers interact with each other through public grids or trusted third intermediary. With Blockchain, a decentralized system of buying and selling energy can be established. It could be also adopted for products retail, real estate and similar commercial activities.

- The intelligent transportation industry [89]–[91] is evolving because of Blockchain. The technology aids in implementing a secure and trusted ITS infrastructure based on peer-to-peer networks. Blockchain-based ITS applications enable drivers and users to set transport conditions as well as securely share and update road and infrastructure status and information without third-party providers. Automatic parking and toll and fuel payment systems are also proposed.

A number of researchers have expressed interest in the application of Blockchain technology to the last cited industry. Their contributions include those related to traffic management, driving safety, road safety and security, payments and billing, parking services, privacy, and preserving security for ITS. In the next section, a detailed overview of existing related studies is presented.

III. HISTORY OF BLOCKCHAIN

The history of Blockchain technology relates to its beginnings and evolution leading to Bitcoin, Ethereum, and Hyperledger implementations. As illustrated in Figure 10, three basic periods are distinguished. First, the pre-Bitcoin period involving cryptographic science and related areas. Second, the Blockchain 1.0 phase includes the first implementation of Bitcoin, a well-known financial application. Finally, in the Blockchain 2.0 phase, more elaborate Blockchain platforms, specifically Ethereum and Hyperledger, are announced.

A. PRE-BITCOIN

Some research initiatives [36], [92]–[95] associated the Blockchain technology with the emergence of Bitcoin, which was proposed by Nakamoto in 2008 [28]; however, the concept existed prior to that. In 1991, the preliminary work of Haber and Stornetta focused on the cryptographic security chain of blocks [96]. Their idea was to implement an anti-fraud system against data timestamp tampering. In 1998, Szabo *et al.* [97] proposed a decentralized digital currency mechanism called "bit gold," presenting an introduction to what is subsequently called "Bitcoin." However, "bit gold" was never implemented. After two years, Stefan Konst published a unified theory of encryption protection chains including some applications [98]. In 2008, Satoshi Nakamoto published his white paper "Bitcoin: A Peer-to-Peer Electronic Cash System" [28] in which he proposed a new form of digital currency; Bitcoin was implemented in 2009. From

then on, this technology evolved, leading to the more generic Blockchain 2.0 that deals with applications beyond cash transactions and currencies. In 2015, smart contracts and Ethereum Blockchain [48] emerged.

B. BLOCKCHAIN 1.0

The Blockchain 1.0 phase refers the launch of Bitcoin Blockchain application. In this section, the Bitcoin standard, consensus protocols, and reward mechanism for miners are explored.

1) BITCOIN

Bitcoin [92] is a public, decentralized, and fully distributed peer-to-peer system for digital currencies. Originally designed by Satoshi Nakamoto (pseudonym), Bitcoin aimed to create an electronic cash solution sheltered from any central authority for validation or settlement of transactions and currency insurance. Different from traditional currencies, it is entirely virtual; no physical or digital coins are handled. Bitcoin users possess keys that prove ownership rights in the network. Users sign transactions with their keys to unlock and spend the value by transferring it to another key owner. Keys are typically registered in a digital wallet on user terminals. Bitcoin relies on a robust computation process called ''mining,'' which verifies and unanimously validates a transaction every 10 min (on average); then, the miners are rewarded. Because of Bitcoin, the problem of double-spent transactions of digital currencies [99] has been resolved.

2) CONSENSUS PROTOCOLS

Consensus protocols present the core of Blockchain technology. Their main role is to maintain and verify transactions across a distributed network that is not fully trusted using cryptographic mechanisms. Moreover, consensus nodes are able to validate transferred data even by approval or declines. Validated data are also orderly appended into the Blockchain register. The majority of the known studied consensus protocols published in the literature are presented in the following section.

a: PROOF-OF-WORK

Proof of work (PoW) is among the most widely used consensus mechanism in existing Blockchains [100]. Each modification of single-chain elements requires subsequent changes in all upcoming elements to ensure validity. Accordingly, an attacker who intends to modify the contents of a block must also change the rest of the chain's hash code, which is difficult to accomplish [101]. Consequently, this mechanism enhances the Blockchain security. The PoW mechanism is regarded as a mathematical puzzle because the first miner who finds the solution is permitted to publish the block. Some puzzles are extremely heavy in a computational sense because they require performing numerous computations to solve them. Therefore, miners with advanced computational capabilities have better chances. To summarize, the probability of solving the puzzle first corresponds to the miner's proportion of work and contribution. This property is labeled as progress-free. Thus, the number of blocks created is proportional to a miner's contribution to the solution of the puzzle [102]. The consensus mechanism is the extension of the branch with the most supporting computations. The longest branch is that with the most work behind it when blocks are mined with the same interval and puzzle difficulty. Consequently, the consensus mechanism leads to a long-term consensus chain.

b: PROOF-OF-STAKE

Proof of stake (PoS) [103], [104] represents a consensus mechanism based on a proof of ownership (i.e., the stake); rigorous computational work is not required [105], [106]. Using PoS, which involves a few algorithms, miners proportionally mine blocks according to their stake [107]. The PoS mechanism is comparable to PoW because miners directly mine blocks in proportion to their wealth instead of using money. Similar miners may also mine with the same probability proportionate to their stakes. Thus, a similar miner is chosen to propose a block if the selected miner does not accomplish it on time [108].

c: DELEGATED PROOF OF STAKE

As an extension of PoS, the delegated PoS (DPoS) [49], [53] is a dependable and verifiable transaction approval protocol based on a shareholder voting scheme. By distributed vote, the DPoS algorithm chooses contributor nodes that can play as witnesses and delegate roles in the validation process. Elected witnesses are called to generate blocks regularly at defined time slots. Delegates nodes are in charge of deciding or modifying Blockchain parameters, such as intervals of blocks, sizes of transactions, transactions fees, and transactions per block. To ensure that reputation is maintained, non-trusted nodes may be progressively rejected. Compared with PoS, the DPoS mechanism [54] saves more energy and accelerates transactions rates.

d: PRACTICAL BYZANTINE FAULT TOLERANCE (PBFT)

The practical Byzantine fault tolerance (PBFT), originally introduced in the late '90s by Miguel Castro and Barbara Liskov [109], is an asynchronous algorithm for efficiently processing transactions and ensuring reliability by double-checking the information with the message queue server. The PBFT mechanism [53] protects against system failures through collective decision-making (both correct and faulty nodes) with the goal of reducing the influence of faulty nodes. The PBFT algorithm is derived from the Byzantine generals problem [110], [111]. The PBFT mechanism enables a distributed computer network to function as desired and correctly reach a sufficient consensus despite the failure of malicious system components (nodes) or the propagation of incorrect information to other peers.

e: PROOF OF ELAPSED TIME

Often used on permissioned networks, proof of elapsed time (PoET) [49] is a scalable, nimble, and energy-efficient

consensus protocol designed by Intel's Sawtooth project. It is based on random block generation by reducing the high utilization of processing resources or coins, thus avoiding greedy energy consumption. Because all participant nodes have equal chances to be a miner, PoET follows a fair mechanism for selection. Specifically, all nodes are given a random waiting time during which they are on standby. A node that finishes its waiting time first is then selected to generate the block. The PoET protocol ensures that the waiting time assignment among nodes is purely random. It must be verified that the winner node has certainly completed its waiting period. To keep the environment protected, PoET requires mutual trust [112].

f: PROOF OF ACTIVITY

Proof of activity (PoAc) [49] is a consensus algorithm for decentralized systems. The PoAc algorithm is a hybrid protocol that combines block generation through the PoW mining mechanism and validation by the PoS mechanism.

g: PROOF OF BURN

Proof of burn (PoB) [49] is a consensus algorithm for state agreement and validation of Blockchain networks. It is considered as a PoW alternative that aims to prevent the double spending of cryptocurrency coins. To become a validator block node, coins must be paid. In contrast, validated coins are burned or destroyed. Because the validation process is costly, PoB avoids the unnecessary waste of money and resources.

h: PROOF OF CAPACITY

Proof of capacity (PoC) [49], also known as proof of space and proof of storage, is an energy-saving consensus protocol. To gain the next block production, a concurrent validator node has to engage hard drive spaces to host outcome data named ''plots.'' In addition, PoC does not require expensive hardware (called application-specific integrated circuit, which is next in the evolution of crypto-mining after central processing units and graphic processing units). It is capable of accomplishing the same task in a considerably more efficient and profitable manner [113].

3) MINING INCENTIVES

Blockchain security is based on incentives for miners to follow the protocol. Incentives are offered to generate and validate blocks with appropriate transactions issued by the network and to work on the branch supported with the most work. An example of this is a monetary incentive. Miners are rewarded for mining blocks that lead to a long-term consensus chain [36]. In contrast, the miners are penalized if they do not comply with this rule. The penalization in PoW involves reducing the power necessary for computations [108], whereas in PoS, the penalization occurs through the stake [103], [107]. Without penalization, miners may opt to mine on different chains simultaneously and collect rewards; this can increase the profitability of mining malicious blocks. This is known as a nothing-at-stake problem, considering that the miner does not lose anything by mining different chains [107], [114]. Therefore, penalization for mining on blocks that are not the part of the final Blockchain is necessary. Due to incentives and penalizations, the profit of miners from mining on the blocks is expected to be a part of the true Blockchain. Because the majority is honest, the honesty of a node is profitable [36], [105]. The rationale behind PoS is that stakeholders find their stakes important; thus, they receive incentives for securing the system [107]. Furthermore, monetary incentives ensure that prescriptions are followed. Business and social incentives, such as a consortium with known participants running the Blockchain, can also be offered. Incentives contribute to honest business and social relationships, ensuring successful collaborations.

C. BLOCKCHAIN 2.0

The Blockchain 2.0 phase refers to the birth of Blockchain applications beyond the digital currency exchange. This section discusses the wide range of Blockchain implementations, such as Ethereum, Hyperledger, and related areas, developed after Bitcoin.

1) SMART CONTRACT

A smart contract represents an executable piece of code that may reside on Blockchain such that the script can be inspected by all participants. The smart contract is comparable to stored procedures in conventional relational databases; the difference is that the former resides in Blockchain [115]. Therefore, a stored procedure is not necessarily enforced. However, bypassing the smart contract is not possible [116]. It is executed on all nodes; hence, each node runs a virtual machine. Accordingly, Blockchain represents a distributed virtual machine. Considering that the code is executed on every node, avoiding inconsistencies by having a precise and deterministic contract is necessary. Hence, the smart contract [93], [116] is an autonomous actor that behaves transparently and predictably.

2) ETHEREUM

Blockchain technology has been applied to various applications labeled as Bitcoin 2.0, Blockchain 2.0, and Crypto 2.0. Ethereum [117], Established in 2015, it is the biggest open-ended decentralized software platform (ĐApps). It enables creating and running applications without fraud, downtime, interference, or control from a third party. It also represents a Turing-complete programming language based on Blockchain. Developers use it for building and publishing distributed applications. Ethereum applications are diverse and run on its platform-specific cryptographic token, Ether. Ethereum launched a pre-sale of Ether in 2014 and received considerable attention from developers that are interested in formulating and running applications based on Ethereum. The use of Ether is twofold. First, it is used to trade a digital currency exchange similar to other cryptocurrencies.

TABLE 3. Hyperledger frameworks for Blockchain technology.

Frameworks	Definition and properties
Hyperledger Burrow	It is a fully-fledged Blockchain node that runs Ethereum Virtual Machine (EVM) and Web Assembly (WASM) smart contracts.
Hyperledger Fabric	Intended as a foundation for developing applications or solutions with a modular architecture. It allows consensus and membership services as plug-and-play components,such as consensus and membership services, to be plug-and-play.
Hyperledger Indy	It uses the concept of Self Sovereign Identity and Blockchain technology to protect digital identities from threats.
Hyperledger Iroha	It was developed by a group of developers in Japan who built their own Blockchain technology for some mobile use cases. It is implemented in C++, which can be more performant for small data and focused-use cases.
Hyperledger Sawtooth	It was originally developed by Intel and introduced a novel consensus algorithm called PoET.
Hyperledger Caliper	It is a Blockchain performance benchmarking framework that enables users to test different Blockchain solutions with custom-use cases and derive a set of performance test results.
Hyperledger Cello	It provides an on-demand deployment model of the Blockchain system where a real-time dashboard is provided to users to check the Blockchain system status and statistics (e.g., events, system performance, and utilization).
Hyperledger Explorer	It is a viewing dashboard that enables the network information control of transactions, blocks, logs, etc.

Second, it is used within Ethereum to run applications and monetize the work. As defined by Ethereum, it is employed to ''codify, decentralize, secure, and trade just about anything.'' Ethereum's big project is Microsoft's partnership with ConsenSys [78] offering ''Ethereum Blockchain as a Service (EBaaS)'' on Microsoft Azure [118].

3) HYPERLEDGER

Hyperledger [39], [119] began in 2015 under the Linux Foundation. The idea was to create an open-source Blockchain technology that can enable individuals, businesses, and interested parties to collaborate. It is a modular, highly secure, and interoperable distributed ledger solution involved in concrete domains, such as banking, financial services, and healthcare. The Hyperledger project emerges from a set of frameworks and tools, as summarized in Table 3.

As a framework example, Hyperledger Burrow [44], [119] presents a strongly deterministic and permissible smart contract machine that offers both access control and authorization layers to clients. Originally developed by Monax [120] in 2017, it was classified as the fourth distributed ledger platform within Hyperledger. Another framework is called Hyperledger Fabric [45], [119], which is a modular, scalable, and flexible platform for developing permissioned distributed ledger solutions. Its ability to support varied consensus protocols renders it suitable for different trust models and use cases. Compared with others platforms, Hyperledger Fabric does not require a specific coding language for a specific domain or cryptocurrency to run applications; in fact, it is called a general-purpose programming language platform. It enables the formation of participant channels for creating separate ledgers where transactions are hidden from other participants in the same private network. This is useful in case competing participants are present. Furthermore, it allows portable membership for permissioned models. Another distributed ledger with a decentralized identity is Hyperledger Indy [47], [119]. It allows the creation of digital and interoperable identities and uses distributed ledgers or Blockchains. Hyperledger Indy satisfies the requirements of privacy and self-sovereignty of identity. Identity claims could be verified by combined or individually secured transferred information, such as passport, birth certificate, and driver's license. Hyperledger Iroha [32], [119], which is an easy incorporated-in-project distributed Blockchain framework, is also introduced. It was originally developed by Soramitsu and proposed by Soramitsu, Hitachi, NTT Data, and Colu. It has a simple structure, enables mobile application development, and uses new chain-based Byzantine fault-tolerant consensus algorithm. Another proposed solution, Hyperledger Sawtooth [51], [119] is a modular framework aiming to preserve the distributed structure of ledgers and safety of smart contracts. It allows organizations and user groups to evaluate their Blockchain applications and enables dynamic consensus in which consensus algorithms can easily change. In addition, it supports the PoET consensus protocol and is compatible with Ethereum contracts. The parallel execution of transactions is enabled, and their privacy is preserved. Hyperledger Caliper [119], [121] is another open-source framework from the Linux Foundation that uses utility libraries and tools provided by Hyperledger. It is a performance evaluation tool for Blockchain implementation that is compatible with multiple Blockchain platforms. It is used as a transaction latency indicator and transactions-per-second indicator; it also measures resource utilization and others metrics. Furthermore, Hyperledger Cello [119], [122] is another toolkit providing an on-demand deployment model of a Blockchain system. A real-time dashboard is provided to users to check the Blockchain system status and statistics (e.g., events, system performance, and utilization) as well as manage Blockchain and chain codes; Python and

TABLE 4. Features comparison of the well-known Blockchain technologies: Bitcoin, Ethereum and Hyperledger.

	Bitcoin	Ethereum	Hyperledger
Type	Public	Public / private	Private
Application	Crypto-currencies	General platform	General platform
Blockchain platform	No	Yes	Yes
Source	***	Open source Ethereum Foundation	Open source Linux Foundation
Consensus algorithm	PoW	PoW, PoS	PBFT, others
Language	C++, Golang	Solidity, LLL, Serpent	Java, Golang
Currency transaction rate	Lower	Higher	No
Data exchange rate	No	Low data volume	High data volume
Energy saving	No	No	Yes

JavaScript are its main programming languages. Finally, the Hyperledger Explorer toolkit [119], [123], which is a viewing dashboard, enables the network information control of transactions, blocks, logs, etc. This tool is compatible with open-source, commercial, authorization, or authentication platforms. Most of these tools support the Hyperledger Fabric Blockchain infrastructure.

4) COMPARISON BETWEEN BITCOIN, ETHEREUM AND HYPERLEDGER

Table 4 summarizes the details of the most popular Blockchain platforms: Bitcoin, Ethereum, and Hyperledger [124], [125]. Features, such as Blockchain types (public/permissionless, consortium, or private/permissionless), adequate consensus algorithms (PoW, PoS, PBFT, etc.), and suitable applications (currencies, smart contracts, etc.), are found to differ from one Blockchain environment to another. Bitcoin was the first popular Blockchain implementation. It is a public Blockchain that uses a stack-based language and a secure hash algorithm, such as SHA-256. Bitcoin primarily acts as a store of value and a medium of payment transactions; however, the transaction rate per second is limited. In addition, Bitcoin adopts the PoW algorithm for consensus operations that requires high-computational performance. Ethereum allows developers and clients of the enterprise to access a single-click cloud-based Blockchain developer environment. Similar to Bitcoin, Ethereum is enabled by the principle of distributed ledgers and cryptography; however, its programming language is Turning-complete, and it uses Ethash as a secure hash algorithm. The purpose of Ethereum is to enable peer-to-peer contracts and applications through its currency vehicle; it is not intended as a payment alternative. Its main objectives are to facilitate and monetize developers who build and run ĐApps [126]. Ethereum enables a higher transaction rate in both private and public Blockchains. In addition to the PoW, it supports the PoS consensus algorithm to a moderate required computational complexity to enhance performance. For these reasons, Ethereum presents a better solution for limited computational capacities and environments with higher transaction rates. Hyperledger aims to provide a more improved Blockchain environment. It is a Linux open-source platform designed for business applications. The Hyperledger Fabric presents the commonly used Hyperledger framework implemented on a private ledger. It supports more sophisticated consensus algorithms, such as PBFT, PoW, and PoS. It can ensure high transaction volumes at approximately 3500/s, rendering it suitable for applications with high data volume. It also supports simple access control mechanisms. Different from Bitcoin and Ethereum, the Hyperledger Fabric is not recommended for cryptocurrencies, such as public transactions or incentive approaches, because it is based on a permissionless environment.

IV. IoV-LAYERED ARCHITECTURE MODELS

This review examined the most significant contributions of Blockchain in IoV, utilising the IoT architecture layer. The taxonomy of IoV architectures and their different layers are presented in this section. To the best of knowledge of the authors, an exact definition of the IoV architecture model has not been reported in literature. Researchers define a wide range of IoV architectures, from simple to elaborate layered models, as shown in Figure 11.

A. THREE-LAYERED IoV ARCHITECTURE

The three-layered model [127], [128] introduces the fundamental level of the IoV architecture where the majority of research in IoT architecture starts. The perception layer, also named as sensing layer, presents the interface with the IoV environment that collects and communicates the events that occurred on the upper network layer. The network layer presents the connection point that transfers collected data through access networks, such as LTE, Wi-Fi, and Bluetooth, to the application layer. The latter presents the decisional level that processes the received data using tools, such as computational, statistical, analytical, or storage services.

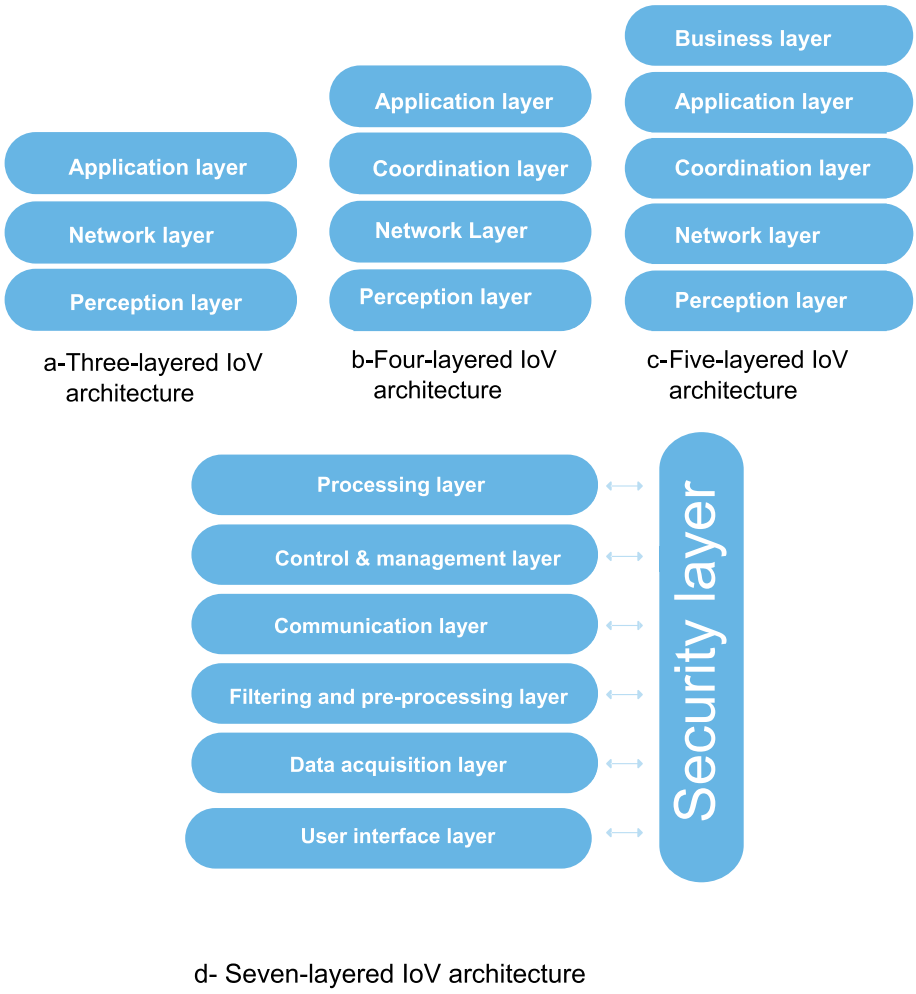


FIGURE 11. Existed IoV layered architecture models.

B. FOUR-LAYERED IoV ARCHITECTURE

The four-layered model [129] introduces additional functionalities to the network layer, including control networks, data management (analysis, processing, etc.) and monitoring, and node management. This model also adds a coordination layer responsible for intelligent data processing and computing as well as resource allocation. However, the model does not particularly define the sets of functionalities for upper layers, especially for data management.

C. FIVE-LAYERED IoV ARCHITECTURE

The five-layered model [130] presents a global and clearly defined model where the majority of IoV functionalities are included. The intermediate ''network and transport'' and ''coordination'' layers of the previous model are merged into a single layer, called ''coordination'' layer, in the five-level model. Its main role is to secure the transportation of data through existing heterogeneous networks. Data management, including storage, analysis, processing, and decision-making, is associated with the artificial intelligence layer. Efficient remote solutions for data management, such as cloud computing, are applied if the integrated computational resources of IoV nodes are restricted and insufficient. The application layer introduces smart vehicular services to end-users, and the business layer offers a practical display of results, such as flowcharts, tables, and graphs, which are provided by the lower layer. This top layer aids in determining the best business model or strategy.

D. SEVEN-LAYERED IoV ARCHITECTURE

Although the five-layered IoV architecture model [131], [132] is regarded as the most structured, it has some gaps. These deficiencies include the lack of a security layer (which ensures the smoothness and security of IoV functionalities of different levels) and communication layer (which smartly selects the best transmission channel if many heterogeneous networks are available (satellite, mobile network, WiFi, etc.)). To enable the robustness of such a model, the addition of pre-processing and filtering layers reduces the load of the upper layer by avoiding the transmission of redundant or unnecessary data; all of these aspects have been considered by the seven-layered model. In the following, each layer is described. The user–vehicle interface is responsible

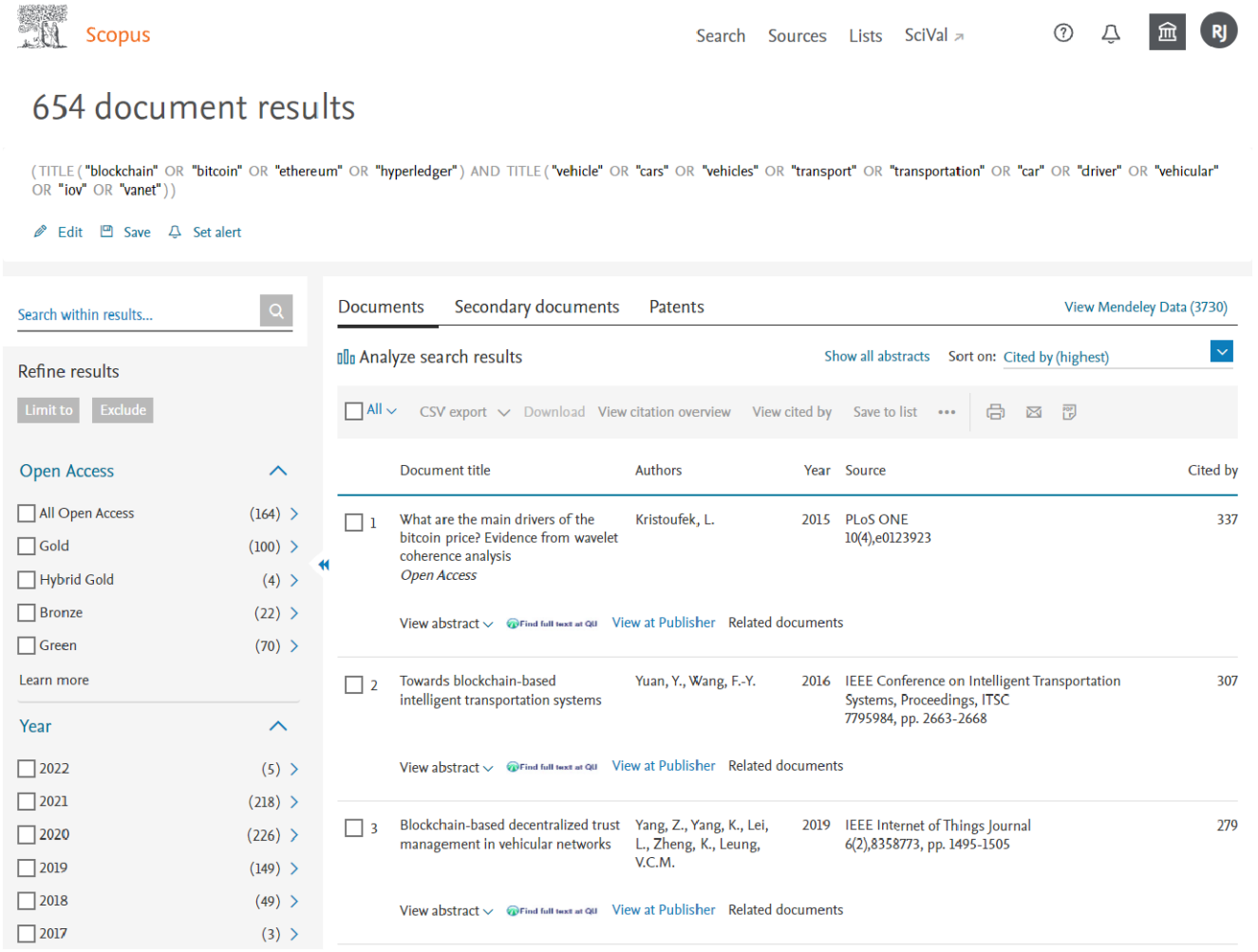


FIGURE 12. Scopus - document search results.

for notifying vehicle drivers about events that occur in the IoV environment due to vibrations and sound or light signals. The data acquisition layer collects data regarding these events. The data-filtering and pre-processing layer analyzes the collected information and eliminates useless and redundant data. The communication layer employs appropriate metrics to identify the suitable heterogeneous network for transferring filtered data. As its name suggests, the control and management layer provides control and management mechanisms, such as data packet inspection, flow-based management, and policy enforcement. The processing layer computes the output of the received data according to predefined procedures and prepares the results for end-users. Finally, the security layer transversely interacts with all the aforementioned layers. Its main function is to ensure security at all levels, including privacy, confidentiality, authentication, non-repudiation, integrity, and security (against attacks). In the following, our review of research work and efforts devoted to the application of Blockchain to IoV is based on the seven-layered IoV.

V. STATE OF THE ART LITERATURE CONFERENCES: CLASSIFICATION METHODOLOGY, STATISTICS AND DISCUSSION

In this paper, we present useful statistics regarding research progression published in the Scopus database [133]. As shown in Figure 12, we found 654 research papers in executing the following search request.

allintitle:
(Blockchain | Bitcoin | Ethereum | Hyperledger) (Vehicle | Cars |Vehicles |Transport | Transportation | Car | Driver | Vehicular)
Source: Scopus

The number of published papers in 2020 is 226 (the highest at the time of writing this paper), as indicated in Figure 13. The publishers are from well-ranked journals and conference proceedings, such as IEEE Access, IEEE Internet of Things Journal, IEEE Transactions on Vehicular Technology, IEEE Transactions on Intelligent Transportation Systems, Computers, and Electrical Engineering. This indicates that

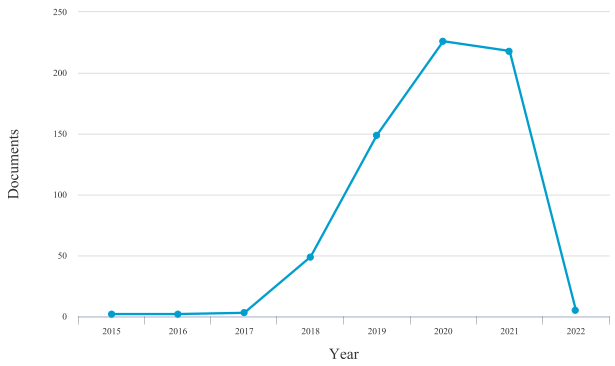


FIGURE 13. Documents per year.

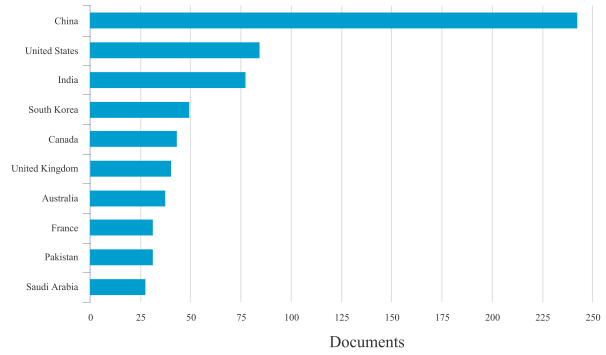


FIGURE 14. Documents by country.

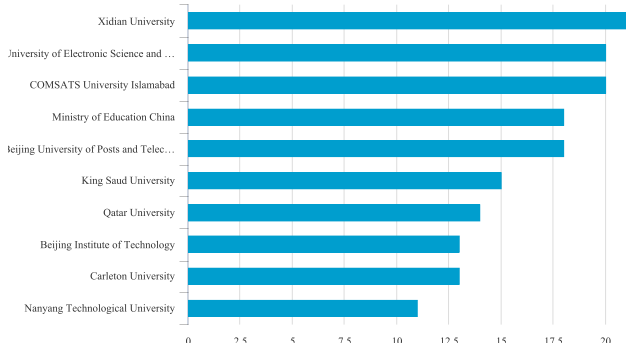


FIGURE 15. Documents by affiliation.

Blockchain technology is an attractive research focus in scientific communities.

Figures 14 and 15 show that most of the published research works are produced by Chinese institutions with a total of 242 publications.

The top Chinese institutions are the Xidian University, University of Electronics Science and Technology of China, Beijing University of Posts and Telecommunications, and Beijing Institute of Technology. The United States is second with more than 84 published papers, followed by India with 77 publications. South Korea, Canada, UK, Australia, France, Pakistan, and Saudi Arabia are also contributing countries (listed according to their number of contributions). According to the Scopus database, N. Javaid from COMSATS University Islamabad in Pakistan, Y. Zhang from Texas A& M University in USA, and M. Guizani from Qatar University are the authors with the most contributions in the field considered in this paper. To provide an overview on current research trends, Table 5 lists the first five highly cited papers (excluding literature reviews); publication year, publisher source, authors, and country are summarized.

Yong Yuan and Fei-Yue Wang in [36] discusses the potential integration of Blockchain technology in transportation research. It also presents a seven-layered conceptual model that aids in standardizing a typical Blockchain-based ITS architecture. Yang *et al.* in [134] presents a decentralized trust management system in vehicular networks based on Blockchain techniques. In this system, vehicles can validate received messages from neighboring vehicles using a Bayesian inference model. Lei *et al.* in [105] contributes to the improvement of security for vehicular communications systems. More specifically, it proposes an efficient and secure key management framework applied to heterogeneous ITS and implemented at the top of a distributed Blockchain-based network. Sharma *et al.* in [135] proposes a Block vehicular network (Block-VN) architecture for a distributed and secure network for vehicles using Blockchain. This solution enhances the decentralized transport management system. Li *et al.* in [101] proposes the CreditCoin solution that utilizes Blockchain to preserve the privacy of user identities in a distributed vehicular network. It encourages users to participate in sharing traffic data via incentive mechanisms.

Our review methodology involves the collection of all documents pertaining to Blockchain in IoV systems from the Scopus database [133]. The selected papers were found according to the following set of keywords: Blockchain, Bitcoin, Ethereum, Hyperledger, Vehicle(s), Car(s), Transport, Transportation, Driver, Vehicular; a total of 654 papers were found. Then, papers on economy and other articles that were not relevant to the proposed review were omitted. The studies were categorized according to their research direction, as shown in Figure 16. Six categories were identified: 23% focused on the security aspect, 17% on transport applications, 10% on energy, 25% on communication and networks, 19% on data management, and 5% on payment and optimization. In the following, the research contributions by category projected on the seven-layered IoV architecture model are discussed; Table 6 summarizes all of the reviewed research works.

A. SECURITY

Security issues are critical in vehicular networks because of their sensitive effects on the user. Security failures, hacker threats, and cyber attacks may result in vehicle immobilization, road accidents, financial losses, disclosure of sensitive data, and even endangerment of road-user safety. Many contributions were proposed to enhance data security in this field, aiming at establishing and improving privacy, anonymity, authentication, trust, resilience to attacks, reputation, immutability, confidentiality, integrity, accessibility, identification, transparency, and credibility. A trustworthy and credible distributed Blockchain-based platform for

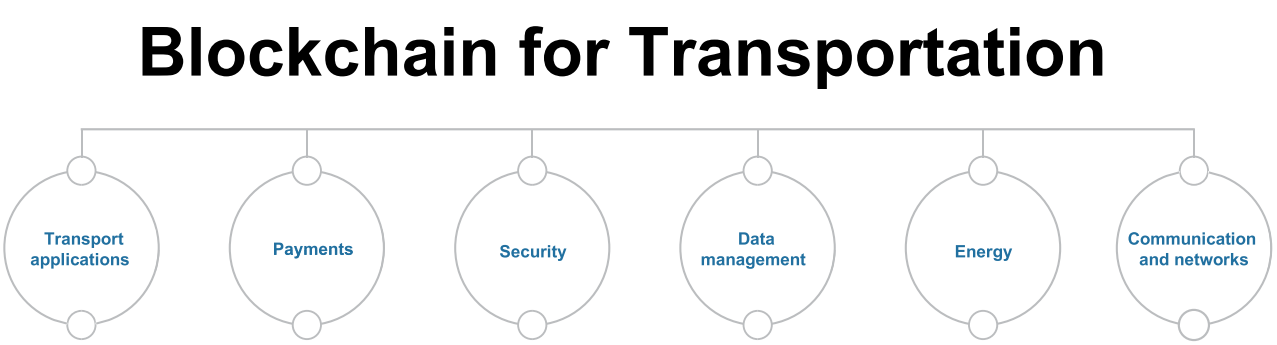


FIGURE 16. Blockchain for transportation.

TABLE 5. First five highly cited research works.

Year	Title	Publisher source	Authors	Country
2016	Towards Blockchain-based intelligent transportation systems	IEEE Conference on Intelligent Transportation Systems	Y. Yuan et al.	China
2019	Blockchain-based decentralized trust management in vehicular networks	IEEE Internet of things Journal	Yang Z.et al.	China
2017	Blockchain-Based Dynamic Key Management for Heterogeneous Intelligent Transportation Systems	IEEE Internet of Things Journal	A. Lei et al.	UK
2017	Bloc-VN: A distributed Blockchain based vehicular network architecture in smart city	Journal of Information Processing Systems	P.K. Sharma et al.	South Korea
2018	CreditCoin: A Privacy-Preserving Blockchain-Based Incentive Announcement Network for Communications of Smart Vehicles	IEEE Transactions on Intelligent Transportation Systems	L. Li et al.	China, KSA

vehicular systems is proposed in [134]. Using a Bayesian inference model, a vehicle can validate messages from nearby vehicles. The vehicle can rate each message from source vehicles based on the validation result. Roadside units (RSUs) calculate the trust value offsets of involved vehicles and store them in a ''block.'' Once this is achieved, each RSU attempts to add their ''blocks'' to the trusted Blockchain. The performance of the proposed solution was evaluated by focusing on security and privacy; other properties, such as execution time and cost, were not considered. CreditCoin, a privacy-preserving announcement architecture, was studied in [101] to allow and encourage message broadcasting while preserving identities. Users were incentivized to sign and forward messages using the anonymous message aggregation protocol and a Blockchain-based incentive mechanism.

However, note that in this work, Bitcoin has been adopted as a Blockchain implementation platform. Bitcoin is primarily used to buy and sell commodities in a secure pseudo-anonymous marketplace. Hence, it does not support the development of smart contracts and programming features for solving computational problems to facilitate the transfer of various sensitive data. A new reputation system for data credibility assessment based on the Blockchain was proposed in [136]. The proposed Blockchain approach allowed vehicles to evaluate the transmitted data based on their observations of the system. Then, a score value stored in a block was provided to the shared data. Based on the score, vehicles could verify the reputation of sending vehicles and the credibility of sent data. In [137], a smart car authentication and revocation framework was designed with the objective of using Blockchain features to provide updates regarding the status of revoked vehicles and reduce the cost of processing and communications compared with that of a trusted-authority central architecture. A study that focused on the use of Blockchain technology to aid in ensuring and enforcing the authentication of transmitted data and vehicle identity was conducted in [138]. It proposed a mechanism for authenticating vehicle identification and data through data packets transmitted from one vehicle to another using Blockchain technology. Another prototype was presented in [139] to demonstrate how Blockchain technology could ensure transparency in an IoT-based distributed system; the paper proposed a traceability information system. This system collects data, such as sensor data from IoT devices, throughout the manufacturing process and makes the information available to end-users as an added value. A trusted vehicle platform that distinguished between misbehaving and malicious vehicles was proposed in [140]. Using Blockchain, the collection of VANET environmental data, validation of packets, and participation of vehicles in generating and sharing blocks allow vehicles to gain or lose the trust of other vehicles. This platform also performed well in detecting Sybil attacks [141]. A secure and transparent framework for CAVs was proposed in [142]. Blockchain was employed to extract and store data. It reduced the risks of sharing data with fake users, receiving altered information, and compromising the smart sensors of connected vehicles. In [143], a Blockchain-based authentication mechanism using asymmetric keys and a message authentication code was proposed to improve privacy and authenticate messages for VANET. To aggregate the consensus on message authentication, PBFT and PoW were used. A fog node-based distributed Blockchain cloud

architecture scheme was studied in [144] to ensure the privacy of vehicular data and protect them from attacks. The proposed solution was capable of efficiently managing the huge amount of generated vehicle data with high computational performance at the edge of the network.

B. TRANSPORT APPLICATIONS

The smart transport applications for IoV and vehicular systems present a wide, renewed, and innovative market. Researchers have proposed and tested APIs for congestion avoidance, traffic safety, in-vehicle entertainment, and mobility services to locate, unlock, and read the odometers of cars across brands. Research initiatives related to transport applications for vehicle systems present varying contributions and are mainly encompassed in the IoV processing layer combined with the IoV security layer for security and privacy purposes. Blockchain-based platforms are used for smart car parking services [241], [452], [453], car leasing [223], training and learning autonomous cars [224], and establishing trusted multiparty insurance [39]. They are also employed for the secure selling and buying of used cars [257] and the transparent dissemination of the usage history of motors for trading [225]. A smart contract-based platform for emerging transport services was proposed in [242]. With this platform, data regarding the privileges of drivers and vehicles are stored, shared, and then deleted after completing the service. To protect the data stored in the built-in restricted resources of smart vehicles, a secure content caching scheme using private Blockchain and deep reinforcement learning (DRL) approach was designed in [269]. A reliable framework for multi-vehicle cooperative positioning corrections with the goal of increasing the accuracy of the global positioning system (GPS) for locating common vehicles was designed in [260]. Additionally, to enhance system security and robustness, a Blockchain architecture was utilized to link sensor-rich vehicles, common vehicles, and RSUs. The simulation results demonstrate the accuracy, robustness, and security of the framework in terms of vehicular positioning, data transfer, and data sharing, whereas scalability, privacy, execution time, and cost were not analyzed. A credible traffic management mechanism must be capable of intelligently switching traffic lights, quickly allocating the duration of green lights, and ensuring road traffic safety. A proposed system that applies a group signature algorithm and ElGamal encryption algorithm to disable the transmission of malicious and fake messages among vehicles in a consortium was developed in [263]. The performance evaluation results show that the encryption, signature, verification, and batch verification algorithms of the proposed system are superior to other algorithms and have lower computational costs, demonstrating the effectiveness of the proposed scheme.

C. ENERGY

With the introduction of smart cars (i.e., fully autonomous or driverless cars and electric vehicles (EVs)), considerable efforts were devoted for enabling energy and electric utility providers to digitally monitor, manage, and control the EVs of their customers. The primordial tasks of industries and researchers include retrieving the state of charge and remaining range of an EV battery, scheduling and remotely controlling the charging and discharging processes, optimizing relative pricing costs, and building EV management dashboards. The common application among existing energy studies on IoV [283], [284], [287], [289], [291], [294], [295], [405], [454], [455] are for smart charging or fueling services in vehicular networks using decentralized, private, or consortium Blockchain. As an application example, a simple selection mechanism of the charging unit for EV drivers is developed based on smart contracts [282]. In [293], a scheduling approach for EV charging was proposed considering the battery capacity, the rate or behavior of charging and discharging operations, and the relative cost of charging. This mechanism could be extended to consider other selection criteria, such as actual battery status, traffic congestion, and service delay. Other research works [115], [115], [279]–[281], [286], [288], [290], [292], [297]–[300], [319] focused on designing efficient energy trading frameworks for EVs. In [281], an optimized cost-aware trading energy platform was studied over a consortium Blockchain. This platform applied a contract-based incentive mechanism to respect the preferences of EVs and improve their participation cycle. At the level of the IoV communication layer, a novel distributed architecture for energy trading among specific bidirectional battery vehicles was proposed [311]. In the proposed architecture [115], [314]–[318], an autonomous energy exchange process is allowed; consequently, vehicles with surplus energy may execute a discharging operation to charge vehicles with low batteries. At the level of the IoV security layer, research was conducted to secure energy transactions and protect exchange mechanisms from attacks and security vulnerabilities. For example, In [314], energy exchange was secured using consensus algorithms over a topology composed of EVs and charging units. Smart contracts were also applied to personalize preferences and exigencies for charging services. In [317], the study contribution was based on a proof-of-reputation consensus scheme to secure the delivery of energy in a private Blockchain-based energy vehicular network. An incentive scheme for a price model was also applied to order the charging and discharging processes between energy nodes and energy-restricted nodes. Then, the utility function of the energy exchange process was enhanced to improve the satisfaction experience of users.

D. DATA MANAGEMENT

Smart cars and EVs with embedded computers, GPS receivers, short-range wireless network interfaces, and potential access to in-car sensors and the Internet must be capable of sharing and storing records of events and sensitive data, such as the identity of drivers or vehicles, cryptographic keys, localization, predicted future direction, traffic, and roads congestion. To avoid security vulnerabilities and bottleneck problems in centralized architectures, sharing and storing must

TABLE 6. Papers classified according to research directions and IoV layer correspondence.

Research axis	Research projected to IoV-layered architecture model		
	IoV Processing layer	**IoV Communication layer**	**IoV security layer**
Security	[145], [146]	[147]–[150]	[103], [134], [136]–[140], [142]–[144], [151]–[221]
Transport applications	[39], [222]–[256]	-	[257]–[278]
Energy	[115], [281]–[299], [299]–[310]	[297]–[300], [311]–[313]	[115], [314]–[319]
Data management	[105], [159], [320]–[351]	[268], [352]	[105], [159], [320]–[345], [353]–[366]
Communication and network	[190]–[373]	[135], [157], [158], [237], [374]–[403]	[135], [157], [158], [374]–[397], [404]–[441]
Payments	[102], [107], [108], [442]–[443], [443]–[449]	[104], [106]	[102], [104], [106]–[108], [114], [442], [450], [451]

be securely implemented over a fully distributed or semi-distributed vehicular network topology. As regards works related to the Blockchain-based data management axis [105], [159], [178], [320]–[344], [344], [345], [345]–[348], [353], all contributions reside in both the IoV processing layer and IoV security layer to offer novel traffic services and/or secure the transferred data, thus avoiding the security attack of vehicular systems. Fundamental works [269], [321], [325], [331], [337], [338], [341], [342], [352] propose the use of smart frameworks for generating, storing, and sharing data over existing network elements, including vehicles, users, infrastructure nodes, and sensors, over a consortium or private Blockchain. As a primordial service for improving road safety, especially with the introduction of self-driving cars, a control application for accidents that aided in analyzing and verifying the cause of accidents was suggested in [321]. A privacy scheme was then implemented to prove the correctness of collected and stored events as well as the registry of driver information. In [331], a distributed solution for intelligent vehicular transactions was modeled and studied to overcome the limitations of traditional data management solutions based on a centralized approach. In [341], an enhanced version of the Diffie–Hellman algorithm was proposed to improve trust on the applied verification mechanism in a consortium Blockchain-based network. Moreover, the consensus mechanism was optimized to reduce consensus delays.

E. COMMUNICATION AND NETWORKS

The ability of vehicles to securely communicate among themselves is a key factor for a successful vehicular system. The objective of research works in the communication and network axis [157], [158], [176], [212], [237], [268], [270], [368], [369], [374]–[388], [388]–[400], [442], [456] was to enhance existing or suggest new communication protocols in vehicular networks, such as VANETs [190], [367], [381], [385], IoT based networks [376], IoV [157], [157], [378], [380], [382], [457], UAVs [379], SDN [157], [158], [401], for better security, privacy, trust, reliability, authentication, anonymity, access control, and security against attacks. The contributions were from two major IoV layers: communication and security layers. In [374], a smart and trustworthy communication protocol using Blockchain technology for a cloud vehicular system was proposed. Successful exchanges were achieved as a result of applying an incentive mechanism that improves trust on the implied nodes. Jabbar *et al.* [458] developed a decentralized framework based on Blockchain technology (DISV); the DISV [459]–[461] represents a real-time application specification that provides secure communication among all participants in the transportation system. The developed solution is composed of three layers: perception, network, and application layers. The perception layer assumes the form of an Android application including two sub-systems. The vehicle data collection system [462], [463] is a sub-system for obtaining information regarding the journey and vehicle. The second sub-system, called driver drowsiness detection [464], [465], aims to sense driver drowsiness by acquiring driver behavior information. In [392], a hybrid 5G and cloud vehicle network was studied to support an emergent communication protocol for warning messages while ensuring the privacy of sensitive user information. In [395], a hybrid architecture was developed to secure vehicle-to-vehicle and vehicle-to-infrastructure communications. In [396], a hash-based storage and access control scheme to manage traffic data was proposed for a Blockchain-based vehicular network.

F. PAYMENTS

The payment category presents research works on non-traditional, smart, and decentralized payment and billing solutions for IoV users. It enables secure and efficient transactions, optimized price, and energy consumption. As for the IoV processing layer, an idea on a Blockchain-based billing service that secures transactions between EVs and charging stations was introduced in [107]. Another novel transaction structure for verification and unique ledger registration was proposed for a Hyperledger system to ensure trustworthy and tamper-proof payments [102]. An original optimization model of the distributed scheduling mechanism of EV battery swap stations was studied in [108]. The objective was to optimize the load and cost of power generation. A smart contract-based rental car platform with optimized cost was also proposed in [442]. As for the IoV communication layer, a new topology composed of EVs and charging stations was designed to personalize Bitcoin transactions in a private network and reduce corresponding costs and verification delays [104]. Another optimization approach [106] was conducted to maximize the throughput of transactions in a Blockchain-based IoV network with security and delay

constraints. This approach uses DRL to determine adequate sizes, intervals, and producers of blocks that satisfy imposed constraints. As for the IoV security layer, all the previously cited contributions on different IoV layers [102], [107], [108], [442] used Blockchain technology to secure payments for IoV services and ensure the privacy, reliability, and/or authenticity of transactions and shared data (e.g., payment records, user identities, behaviors, and other sensitive information). For example, certain consensus approaches, such as the PBFT algorithm and smart contracts, could be applied to verify transaction information.

VI. OPEN CHALLENGES AND FUTURE DIRECTIONS

Because BIoV has gained considerable attention from scientists and industries, other emerging technologies, such as machine learning, big data, and 5G, are assumed to contribute to its further development. In particular, the convergence of such technologies and BIoV can lead to the creation of innovative applications and services. Thus, we focus on the challenges confronting Blockchain and propose potential directions to resolve these problems.

A. IMPROVING BLOCKCHAIN PERFORMANCE FOR FUTURE BIoV

The improvement of Blockchain performance is anticipated to be a topic of interest in the near future as the technology is adopted for various applications, including BIoV. Thus, this section focuses on the challenges related to the improvement of Blockchain performance.

1) PERFORMANCE LIMITATIONS AND POSSIBLE DIRECTIONS

Traditional database systems outperform Blockchain in terms of performance due to the latter's peer-to-peer distributed nature. In this section, an overview of the main Blockchain performance limitations that hinder its use in digital interactions is presented.

1) Throughput: Traditional database systems currently outperform the throughput of commercial Blockchain platforms. However, the performance of these platforms must be improved to enable the processing of business transactions in a real-world production environment to be more efficient and effective.
2) Latency: For example, VISA payment service processes 1700 transactions per second on average, whereas Bitcoin processes 4.6 transactions per second [466]. Hence, reducing the processing latency is necessary to preserve security.
3) Network bottleneck: This pertains to any condition under which data flow becomes limited due to insufficient computer or network resources. Because the number of Blockchain systems is increasing, the problem of network bandwidth bottleneck must be resolved.

2) SCALABILITY LIMITATIONS AND POSSIBLE DIRECTIONS

Due to poor scalability and interconnection [467], the development of a Blockchain system for large-scale commercial adoption is problematic. First, traditional Blockchain has a sequential data structure. Accordingly, scalability is hindered because of the sequential block storage. One solution is to develop a parallel data structure that can accommodate multiple chains. Consequently, the addition of multiple blocks to the chain at the same time becomes possible. This enables a faster transaction process and increases throughput. Nevertheless, multiple chains require the enhancement of the consensus protocol to ensure data consistency and integrity. Aelf [468] is a multi-chain parallel computing Blockchain framework based on the concept of the main chain and multi-layer side chains. Its objective is to improve the network capacity and allow the use of Blockchain in commercial applications. Instead of the original chain, Kan *et al.* [469] proposed the introduction of parallel mining and changing the chain data structure to graph chain [470]. Toan *et al.* [471] proposed the use of a consensus mechanism of authorized PoSs to improve the efficiency of the Blockchain network. Fitz *et al.* [472] proposed a parallel-chain composition method to improve settlement latency by combining parallel compositions with a novel transaction-weighing mechanism, demonstrating that reducing the time for a transaction to settle by any given constant while maintaining the same level of security was possible.

3) SECURITY LIMITATIONS AND POSSIBLE DIRECTIONS

Blockchain can be susceptible to distributed DoS (DDoS) attacks although it is regarded as a promising technique for defeating cyber attacks. Because a DDoS attack can consume enormous network resources, it may block legitimate users from responding promptly to service requests. When the DDoS attack targets an insufficiently distributed Blockchain system, the target system may not provide necessary services, including the creation of new blocks and reaching a consensus; this can lead to system failure. Hence, future research must focus on enhancing the security against DDoS attacks. Furthermore, cryptography in Blockchain aims at providing identity security. However, their development in quantum computers can result in the easy breaking of the most widely used encryption. Therefore, research on anti-quantum algorithms must contribute to the enhancement of the cryptography algorithm security, including aggregate, ring, and blind signatures. Furthermore, because Blockchain is based on a code, it is a target for hackers. To improve code protection, researchers must develop a more robust testing standard for Blockchain codes and smart contracts. For example, the smart contract security verification standard (SCSVS) [473] offers guidance for testing all stages of the smart contract development cycle, starting with design and ending with implementation. Third, using the Byzantine fault-tolerant implementations, the security of a Blockchain-based system is ensured when malicious nodes control less than 50% of the mining capacity. As a result, the network is vulnerable to a 51% attack if a malicious node controls at least 51% of the total computing capacity. Furthermore, malicious nodes can manipulate the consensus process and

compel other nodes to remove their transactions. Due to majority control, attackers can spend tokens or coins multiple times (known as double spending).

In this context, innovative consensus protocols were developed as Proof of Participation and Fees [474], Proof of Search [475], Proof of Accuracy [476], Proof of Sincerity [477], Proof of Learning [478], Proof of Benefit [479], Proof of Experience [480], Proof of Evaluation [481], and Proof of Adjourn [482], providing a strong protection that is independent of the hashing capability of attackers. Finally, the investigation of privacy concerns is necessary because protecting sensitive data despite the presence of transparent and open transactions within the public chain is extremely critical. Thus, the challenge is to keep secure algorithms open while protecting data privacy.

B. MACHINE LEARNING WITH BIoV

Machine learning has been established as an efficient approach to support future BIoV. As a basis of artificial intelligence, machine learning [483]–[487] has been used in numerous areas, such as speech recognition, medical diagnosis, and computer vision. It has also revolutionized BIoV services because it enables them to learn from training data and derive data-driven conclusions, provide decision support, and predict improvements in network performance. Thus, interdisciplinary research must focus on the integration of machine learning and BIoV, particularly with regard to designing smart agents and learning-based analysis of the Blockchain-based IoV system. The so-called smart agents are capable of managing the Blockchain system and identifying abnormal behaviors. The detection of abnormal behaviors is critical to the public chain, whereas the proper management of the network is crucial to the consortium and private chains because they require coordination among users. Furthermore, the use of the learning-based analysis of the Blockchain-based system remains limited. Traditional centralized systems do not have considerable amounts of available data for evaluating the performance of the decentralized Blockchain structure. In contrast, learning-based analysis can reveal important information about the mechanism design of Blockchain structures and on-time forecasting models.

- Blockchain must support anonymous data sharing. Users have increasingly become interested in privacy concerns because of the growing number of IoT and wearable devices. Combined with data fusion, the development of Blockchain structures with multiple layers, including sophisticated data authorization for different users, is possible.
- The Blockchain mining activity is technically the same as solving the Markov decision process [488]. Several studies, aimed at determining the optimal mining strategy via single-agent reinforcement learning (RL), were conducted. However, compared with individual mining, pool mining remains prevalent. More precisely, pool mining is performed by miners who collaborate but at the same time compete by mining blocks. Multi-agent RL involves a mixed setting of collaborative and competitive agents. Therefore, it can model the complex pool mining activity and allow miners to determine optimal mining strategies. Cryptocurrency has a critical role in the public chain, and various chains use different cryptocurrencies. Cryptocurrencies and cryptocurrency portfolios have been established as investment options comparable to traditional financial products. Several studies have investigated cryptocurrency price prediction via supervised learning techniques. However, the potentials of RL or DRL have not been fully determined. More importantly, RL and DRL have achieved outstanding performance regarding financial forecasts, such as stock price prediction, considering that historical data do not accurately reflect current market conditions. This results in poor prediction performance with respect to changes in future prices. Thus, the adoption of RL, DRL, or inverse RL is recommended to investigate the investment return of cryptocurrencies.

Another machine learning technique that has been proven promising is federated learning (FL). It is a distributed machine learning approach [489] aimed at achieving collaborative learning using a huge amount of data belonging to different parties; the raw data of different owners are not shared. Cooperative autonomous driving and ITS are future IoV systems that consist not only of an exceptional number of devices but also a considerable amount of privacy-sensitive data. Accordingly, the efficient use of storage, computing, and communication resources is necessary. Direct data-sharing can be prevented by FL; hence, privacy leakage can be minimized. Therefore, FL can be used in resolving current problems and adopted for such applications as road safety prediction, autonomous driving, and vehicular object detection. Because Blockchain is a secure technology, it can tolerate a single-point failure with distributed consensus and support the implementation of additional incentive mechanisms. Thus, participants can be encouraged to contribute to the system effectively [490]. Blockchain is introduced to FL to overcome certain limitations. For example, it can solve the problem that the resiliency of an aggregator depends on the robustness of the center that operates the FL network. In addition, it can prevent vulnerability to malicious clients who can upload poisonous models to attack the FL network. Lu *et al.* [345] developed a novel architecture drawing based on FL to minimize the transmission load and respond to the privacy concerns of providers. The authors proposed a hybrid Blockchain architecture comprising the local directed acyclic graph and the permissioned Blockchain to improve the reliability and security of model parameters. In addition, an asynchronous FL scheme was proposed by adopting DRL for node selection to enhance efficiency. If learned models are integrated into the Blockchain system and a two-stage verification is implemented, then the reliability of shared data is ensured. According to the numerical results, this data-sharing scheme ensures faster convergence and higher learning accuracy. Moreover, Chai *et al.* [252] developed a hierarchical FL algorithm and a hierarchical Blockchain framework to ensure knowledge sharing. In this process, machine learning methods are used to enable the vehicles to learn environmental

data and share the learned knowledge. The hierarchical FL algorithm satisfies the distributed pattern and privacy requirement of IoVs. This hierarchical Blockchain framework can be applied to large-scale vehicular networks. Otoum *et al.* [491] proposed an innovative solution by integrating Blockchain and FL to ensure that network security and data privacy are maintained. This framework is aimed at decentralizing the mutual machine learning models on end devices. To ensure that the shared cloud training can be trusted, a Blockchain-based consensus solution is employed as a second line for privacy protection. In this model, centralized training data and coordination are not necessary to enable end device machine learning; this is achieved using a consensus method in Blockchain.

C. BIG DATA IN BIoV

Due to the rapid progress in BIoV applications, big data analysis has been considered as a vital data analytical tool for maximizing the value of information contained in massive amounts of Blockchain IoV data. In the future, BIoV is expected to experience exponential growth in terms of diversity, velocity, and volume of Blockchain data. Big data analysis enables a variety of solutions, including analytics, data cleansing, and storage, which aid in the implementation of BIoV systems [492]. Additionally, big data analysis enable cleaning services, which are regarded as a pre-processing step prior to big data analytics. This pre-processing step is used to integrate and enhance the quality of big data. In particular, the cleaning service is divided into two distinct stages. Data integration, also known as data aggregation or data fusion, is the initial step. It is followed by data quality management, which is responsible for identifying low-quality information, such as redundant or damaged data (e.g., Blockchain-based sensor networks), in BIoV data gathering services. Moreover, the analytics service [493] includes data analysis, processing methodologies, and models (e.g., MapReduce processing and data clustering techniques). Moreover, data clustering is frequently used to analyze the use and performance characteristics of large peer-to-peer consensus-based systems. In particular, Blockchain datasets (e.g., Bitcoin data) are gathered, analyzed, and visualized to determine previously unknown patterns in Blockchain networks. Additionally, BIoV supports big data analysis in terms of enhanced privacy and data integrity protection, ensuring the secure storage of data analytics in big data. In these circumstances, BIoV [494] is an excellent solution for big data problems. Furthermore, decentralized management maintains the stability and authenticity of Blockchain; in turn, massive data resources are secured. Blockchain technology enables the transparent and trustworthy interchange of large amounts of data between customers and service providers. By eliminating security barriers, BIoV can enable large-scale universal data interchange. Recently, researchers developed various big data models that use Blockchain technology, including solutions for data tracking via Blockchain transactions [495] and data sharing via smart contracts [496]. According to preliminary findings, Blockchain technology [212], [214], [497] has the potential for significantly improving the performance and security of big data applications in the IoV era.

D. BIoV IN 5G NETWORKS AND BEYOND

The mobile industry is developing and preparing to deploy the 5G network, which is anticipated to change businesses and societies. The innovation is based on important benefits, such as massive data interconnection, high system throughput, low operating costs, energy conservation, low network latency, and high data rate. Additionally, the new technology architectures used in 5G wireless networks, such as cloud computing, device-to-device (D2D) communications, network slicing, network function virtualization (NFV), and SDN, have introduced additional security problems [498]. To demonstrate, SDN is prone to security problems, such as the lack of trusted mechanisms between controllers and management applications; attacks on controllers, control plane communications, and switches; and forged and simulated traffic flows [499]. Furthermore, ensuring the integrity of platforms and service providers, as well as avoiding data leakage problems associated with resource sharing between NFV users and servers, remains a challenge [500]. Moreover, Blockchain can be employed to solve the problem of remote data integrity checking when massive data from IoV are uploaded to a cloud server through the 5G network [501]. In addition, Blockchain technology may be able to provide practical security solutions for such problems. For example, Blockchain technology can be leveraged to create decentralized authentication procedures for SDN. As a result, decentralized access authorization through smart contracts can be enabled [502]. Meanwhile, Blockchain can be used to create trust among network elements (e.g., between network users and SDN controllers) and provide secure data transmission and communication. Additionally, Blockchain technology can be employed in NFV to enable network functions and ensure system integrity in spite of data risks, such as data breaches and malicious virtual machine alterations [503]. Similarly, 5G networks support IoT applications through the notion of network slicing, which enables multiple users to share the same physical gear; however, network slicing can create inter-slice security problems. To demonstrate, if multiple slices share a communication link, a malicious user in one slice can detrimentally affect other slices by compromising data or misusing the resources of the target slice [504]. In this case, Blockchain technology can be utilized to construct trustworthy end-to-end network slices and facilitate resource management by network slice providers [505]. When a slice provider requests to construct an end-to-end slice, Blockchain employs smart contracts to secure authentication. As a result, resource suppliers engage in resource trading using contracts that include sub-slice components. During this process, Blockchain technology is utilized to immutably capture and store information on sub-slice deployment. In the context of D2D interactions over 5G networks, Blockchain fosters trust among D2D users and enables them to securely and

transparently exchange data [506]. In a Blockchain-based D2D scenario, the Blockchain mining process is implemented by edge servers and resource devices, such as powerful smartphones and laptops. In contrast, lightweight D2D devices do not require Blockchain mining; they simply connect to the network for communication [507]. Moreover, Blockchain technology is capable of supporting 5G services. To illustrate, due to the immutable and decentralized nature of Blockchain, trust management in 5G mobile vehicular communication is enabled [508]. The 5G VANET strategy utilizes Blockchain technology to identify network attacks and data risks, preventing them from entering automotive ecosystems. In other words, by boosting communication security and reducing computational complexity, Blockchain can enable flexible and secure key management in 5G IoT networks [509]. Blockchain technology, when combined with cloud computing, offers considerable advantages that can be applied to 5G network administration. For example, Blockchain is utilized to create trustworthy end-to-end network slices and renders resource management easier for network slice providers. In [510], the authors demonstrated how vehicle-to-vehicle and vehicle-to-everything communications in vehicular network slices can be dynamically governed using Blockchain. Additionally, the programmable networking of a cloud-native architecture enables the enhancement of 5G network slicing functionalities. For instance, the authors of [511] confirmed that lifecycle slice management can produce, organize, and optimize network slice performance in terms of data throughput, end-to-end delay, and resources due to cloud-native architecture. These findings provide an idea for the next generation of BIoV 5G networks.

VII. CONCLUSION

This paper reviewed the state-of-the-art Blockchain technology studies reported in the literature. The review involves a careful chronological study of Blockchain evolution from the pre-Bitcoin phase (represented by the fundamental cryptographic systems) to the Blockchain 2.0 phase (typified by the use of Hyperledger and the implementation of Ethereum and smart contracts). After identifying the different Blockchain applications in various domains, we focused on intelligent transport applications for IoV networks and classified related research works into six categories: security, transport applications, energy, communication and network, data management, and payments and optimization. Then, for each direction, existing research contributions were classified according to the IoV layers. Most contributions were observed to belong to the three main IoV layers (individual or combined): processing, communication, and security layers. Moreover, we compared this review with previous literature surveys, highlighted its added value, and identified most of the current open problems in Blockchain application.

ACKNOWLEDGMENT

This work was supported by the Qatar National Research Fund (a member of the Qatar Foundation) through the National Priorities Research Program (NPRP) under Grant NPRP11S-1228-170142. Open Access funding provided by the Qatar National Library. The statements made herein are solely the responsibility of the authors.

REFERENCES

[1] S. Tanwar, S. Tyagi, I. Budhiraja, and N. Kumar, "Tactile internet for autonomous vehicles: Latency and reliability analysis," *IEEE Wireless Commun.*, vol. 26, no. 4, pp. 66–72, Aug. 2019.

[2] S. Sharma and B. Kaushik, "A survey on Internet of Vehicles: Applications, security issues & solutions," *Veh. Commun.*, vol. 20, Dec. 2019, Art. no. 100182.

[3] Y. Dai, D. Xu, S. Maharjan, G. Qiao, and Y. Zhang, "Artificial intelligence empowered edge computing and caching for Internet of Vehicles," *IEEE Wireless Commun.*, vol. 26, no. 3, pp. 12–18, Jun. 2019.

[4] A. Lamssaggad, N. Benamar, A. S. Hafid, and M. Msahli, "A survey on the current security landscape of intelligent transportation systems," *IEEE Access*, vol. 9, pp. 9180–9208, 2021.

[5] K. Zheng, Q. Zheng, P. Chatzimisios, W. Xiang, and Y. Zhou, "Heterogeneous vehicular networking: A survey on architecture, challenges, and solutions," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 4, pp. 2377–2396, 4th Quart., 2015.

[6] G. Karagiannis, O. Altintas, E. Ekici, G. Heijenk, B. Jarupan, K. Lin, and T. Weil, "Vehicular networking: A survey and tutorial on requirements, architectures, challenges, standards and solutions," *IEEE Commun. Surveys Tuts.*, vol. 13, no. 4, pp. 584–616, 4th Quart., 2011.

[7] (2021). *ERTICO—ITS Europe*. [Online]. Available: https://ertico.com/

[8] (2021). *Cityverve*. [Online]. Available: https://www.smartsustainablecities.U.K./cityverve

[9] M. Nofer, P. Gomber, O. Hinz, and D. Schiereck, "Blockchain," *Bus. Inf. Syst. Eng.*, vol. 59, no. 3, pp. 183–187, Mar. 2017.

[10] (2021). *Bitcoin.org*. [Online]. Available: https://https://www.bitcoin.org/

[11] A. Reyna, C. Martín, J. Chen, E. Soler, and M. Díaz, "On blockchain and its integration with IoT. Challenges and opportunities," *Future Gener. Comput. Syst.*, vol. 88, pp. 173–190, Nov. 2018.

[12] S. Smetanin, A. Ometov, M. Komarov, P. Masek, and Y. Koucheryavy, "Blockchain evaluation approaches: State-of-the-art and future perspective," *Sensors*, vol. 20, no. 12, p. 3358, 2020, doi: 10.3390/s20123358.

[13] T. A. Butt, R. Iqbal, K. Salah, M. Aloqaily, and Y. Jararweh, "Privacy management in social Internet of Vehicles: Review, challenges and blockchain based solutions," *IEEE Access*, vol. 7, pp. 79694–79713, 2019.

[14] V. Astarita, V. P. Giofrè, G. Mirabelli, and V. Solina, "A review of blockchain-based systems in transportation," *Information*, vol. 11, no. 1, p. 21, Dec. 2019.

[15] R. Gupta, S. Tanwar, N. Kumar, and S. Tyagi, "Blockchain-based security attack resilience schemes for autonomous vehicles in industry 4.0: A systematic review," *Comput. Electr. Eng.*, vol. 86, Sep. 2020, Art. no. 106717.

[16] S. El-Switi and M. Qatawneh, "Application of blockchain technology in used vehicle market: A review," in *Proc. Int. Conf. Inf. Technol. (ICIT)*, Jul. 2021, pp. 49–54.

[17] S. Iqbal, R. M. Noor, and A. W. Malik, "A review of blockchain empowered vehicular network: Performance evaluation of trusted task offloading scheme," in *Proc. IEEE 11th IEEE Symp. Comput. Appl. Ind. Electron. (ISCAIE)*, Apr. 2021, pp. 367–371.

[18] L. Mendiboure, M. A. Chalouf, and F. Krief, "Survey on blockchain-based applications in Internet of Vehicles," *Comput. Electr. Eng.*, vol. 84, Jun. 2020, Art. no. 106646.

[19] M. B. Mollah, J. Zhao, D. Niyato, Y. L. Guan, C. Yuen, S. Sun, K.-Y. Lam, and L. H. Koh, "Blockchain for the Internet of Vehicles towards intelligent transportation systems: A survey," *IEEE Internet Things J.*, vol. 8, no. 6, pp. 4157–4185, Mar. 2021.

[20] X. Wang, C. Xu, Z. Zhou, S. Yang, and L. Sun, "A survey of blockchain-based cybersecurity for vehicular networks," in *Proc. Int. Wireless Commun. Mobile Comput. (IWCMC)*, Jun. 2020, pp. 740–745.

[21] M. Dibaei, X. Zheng, Y. Xia, X. Xu, A. Jolfaei, A. K. Bashir, U. Tariq, D. Yu, and A. V. Vasilakos, "Investigating the prospect of leveraging blockchain and machine learning to secure vehicular networks: A survey," *IEEE Trans. Intell. Transp. Syst.*, vol. 23, no. 2, pp. 683–700, Feb. 2022.

[22] B. Mikavica and A. Kostić-Ljubisavljević, "Blockchain-based solutions for security, privacy, and trust management in vehicular networks: A survey," *J. Supercomput.*, vol. 77, pp. 1–56, Feb. 2021.
[23] S. Megha, H. Salem, E. Ayan, and M. Mazzara, "A survey of blockchain solutions for autonomous vehicles ecosystems," *J. Phys., Conf. Ser.*, vol. 1694, no. 1, Dec. 2020, Art. no. 012024.
[24] N. Khoshavi, G. Tristani, and A. Sargolzaei, "Blockchain applications to improve operation and security of transportation systems: A survey," *Electronics*, vol. 10, no. 5, p. 629, Mar. 2021.
[25] S. Kumar, S. Velliangiri, P. Karthikeyan, S. Kumari, S. Kumar, and M. K. Khan, "A survey on the blockchain techniques for the Internet of Vehicles security," *Trans. Emerg. Telecommun. Technol.*, p. e4317. [Online]. Available: https://onlinelibrary.wiley.com/doi/abs/10.1002/ett.4317, doi: 10.1002/ett.4317.
[26] A. Queiroz, E. Oliveira, M. Barbosa, and K. Dias, "A survey on blockchain and edge computing applied to the Internet of Vehicles," in *Proc. IEEE Int. Conf. Adv. Netw. Telecommun. Syst. (ANTS)*, Dec. 2020, pp. 1–6.
[27] C. Wang, X. Cheng, J. Li, Y. He, and K. Xiao, "A survey: Applications of blockchain in the Internet of Vehicles," *EURASIP J. Wireless Commun. Netw.*, vol. 2021, no. 1, pp. 1–16, Dec. 2021.
[28] S. Nakamoto and A. Bitcoin. (Apr. 2008). *A Peer-to-Peer Electronic Cash System*. [Online]. Available: https://bitcoin.org/bitcoin.pdf
[29] A. Bahga and V. K. Madisetti, "Blockchain platform for industrial Internet of Things," *J. Softw. Eng. Appl.*, vol. 9, no. 10, pp. 533–546, Oct. 2016.
[30] J. Xie, H. Tang, T. Huang, F. R. Yu, R. Xie, J. Liu, and Y. Liu, "A survey of blockchain technology applied to smart cities: Research issues and challenges," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 3, pp. 2794–2830, 3rd Quart., 2019.
[31] H.-N. Dai, Z. Zheng, and Y. Zhang, "Blockchain for Internet of Things: A survey," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 8076–8094, Oct. 2019.
[32] (2021). *Hyperledger Iroha*. [Online]. Available: https://www.hyperledger.org/projects/iroha
[33] M. Pournader, Y. Shi, S. Seuring, and S. C. L. Koh, "Blockchain applications in supply chains, transport and logistics: A systematic review of the literature," *Int. J. Prod. Res.*, vol. 58, no. 7, pp. 2063–2081, Apr. 2020.
[34] S. A. Abeyratne and R. Monfared, "Blockchain ready manufacturing supply chain using distributed ledger," *Int. J. Res. Eng. Technol.*, vol. 5, no. 9, pp. 1–10, Sep. 2016.
[35] J. Yoo, Y. Jung, D. Shin, M. Bae, and E. Jee, "Formal modeling and verification of a federated byzantine agreement algorithm for blockchain platforms," in *Proc. IEEE Int. Workshop Blockchain Oriented Softw. Eng. (IWBOSE)*, Feb. 2019, pp. 11–21.
[36] Y. Yuan and F.-Y. Wang, "Towards blockchain-based intelligent transportation systems," in *Proc. IEEE 19th Int. Conf. Intell. Transp. Syst. (ITSC)*, Nov. 2016, pp. 2663–2668.
[37] (2021). *Blockchain: This is How Bitcoin and Ethereum are Different—Lupus Consultings*. [Online]. Available: https://lupusconsulting.com/2019/01/14/blockchain-this-is-how-bitcoin-and-ethereum-are-different/
[38] (2021). *Bitcoin Blockchain Size 2009–2021 | Statista*. [Online]. Available: https://www.statista.com/statistics/647523/worldwide-bitcoin-blockchain-size/
[39] Z. Li, Z. Xiao, Q. Xu, E. Sotthiwat, R. S. Mong Goh, and X. Liang, "Blockchain and IoT data analytics for fine-grained transportation insurance," in *Proc. IEEE 24th Int. Conf. Parallel Distrib. Syst. (ICPADS)*, Dec. 2018, pp. 1022–1027.
[40] A. Zhang and X. Lin, "Towards secure and privacy-preserving data sharing in e-health systems via consortium blockchain," *J. Med. Syst.*, vol. 42, no. 8, p. 140, 2018.
[41] W. Wang, D. T. Hoang, P. Hu, Z. Xiong, D. Niyato, P. Wang, Y. Wen, and D. I. Kim, "A survey on consensus mechanisms and mining strategy management in blockchain networks," 2018, pp. 1–33, *arXiv:1805.02707*.
[42] Z. Li, J. Kang, R. Yu, D. Ye, Q. Deng, and Y. Zhang, "Consortium blockchain for secure energy trading in industrial Internet of Things," *IEEE Trans. Ind. Informat.*, vol. 14, no. 8, pp. 3690–3700, Aug. 2017.
[43] J. Kang, Z. Xiong, D. Niyato, P. Wang, D. Ye, and D. I. Kim, "Incentivizing consensus propagation in proof-of-stake based consortium blockchain networks," *IEEE Wireless Commun. Lett.*, vol. 8, no. 1, pp. 157–160, Feb. 2019.
[44] (2021). *Hyperledger Hyperledger-Burrow*. [Online]. Available: https://www.hyperledger.org/projects/hyperledger-burrow
[45] (2021). *Hyperledger Fabric*. [Online]. Available: https://www.phyperledger.org/projects/fabric
[46] N. Jirwan, A. Singh, and D. S. Vijay, "Review and analysis of cryptography techniques," *Int. J. Sci. Eng. Res.*, vol. 4, no. 3, pp. 1–6, 2013.
[47] (2021). *Hyperledger Indy*. [Online]. Available: https://www.hyperledger.org/projects/hyperledger-indy
[48] H. Li, R. Lu, L. Zhou, B. Yang, and X. Shen, "An efficient Merkle-tree-based authentication scheme for smart grid," *IEEE Syst. J.*, vol. 8, no. 2, pp. 655–663, Jun. 2014.
[49] M. Andoni, V. Robu, D. Flynn, S. Abram, D. Geach, D. Jenkins, P. McCallum, and A. Peacock, "Blockchain technology in the energy sector: A systematic review of challenges and opportunities," *Renew. Sustain Energy Rev.*, vol. 100, pp. 143–174, Feb. 2019.
[50] (2021). *Hyperledger Quilt*. [Online]. Available: https://www.hyperledger.org/projects/quilt
[51] (2021). *Hyperledger Sawtooth*. [Online]. Available: https://www.hyperledger.org/projects/sawtooth
[52] (2021). *Interledger Protocol (ILP)*. [Online]. Available: https://interledger.org/rfcs/0003-interledger-protocol
[53] D. Mingxiao, M. Xiaofeng, Z. Zhe, W. Xiangwei, and C. Qijun, "A review on consensus algorithm of blockchain," in *Proc. IEEE Int. Conf. Syst., Man, Cybern. (SMC)*, Oct. 2017, pp. 2567–2572.
[54] (2021). *A (Short) Guide to Blockchain Consensus Protocols*. [Online]. Available: https://www.coindesk.com/short-guide-blockchain-consensus-protocolsl
[55] (2021). *Blockchain for Financial Services | IBM*. [Online]. Available: https://www.ibm.com/blockchain/industries/financial-services
[56] (2021). *Home—Abra*. [Online]. Available: https://www.abra.com/
[57] (2021). *How Barclays is Exploring Blockchain | Innovation | Barclays*. [Online]. Available: https://home.barclays/news/2019/7/less-hype-and-more-collaboration–how-barclays-is-exploring-bloc/
[58] (2021). *Press Release: Paypal Launches New Service Enabling Users to Buy, Hold and Sell Cryptocurrency*. Accessed: Oct. 21, 2020. [Online]. Available: https://newsroom.paypal-corp.com/2020-10-21-PayPal-Launches-New-Service-Enabling-Users-to-Buy-Hold-and-Sell-Cryptocurrency
[59] (2021). *Why Mastercard is Bringing Crypto Onto Its Network*. [Online]. Available: https://www.mastercard.com/news/perspectives/2021/why-mastercard-is-bringing-crypto-onto-our-network/
[60] (2021). *Crypto | Money is Evolving | Visa*. [Online]. Available: https://usa.visa.com/solutions/crypto.html
[61] (2021). *Penta Security Systems*. [Online]. Available: https://www.pentasecurity.com/
[62] (2021). *Solidus Labs | Digital Asset Compliance*. [Online]. Available: https://www.soliduslabs.com/
[63] (2021). *Casa | the Most Secure Storage for Your Bitcoin*. [Online]. Available: https://www.keys.casa/
[64] (2021). *Blockchain for Supply Chain—IBM Blockchain | IBM*. [Online]. Available: https://www.ibm.com/blockchain/supply-chain
[65] (2021). *Shipchain Thinks Public Blockchain Can Transform Logistics for Small Business*. [Online]. Available: https://www.forbes.com/sites/robertanzalone/2020/04/20/shipchain-thinks-public-blockchain-can-transform-logistics-for-small-business/?sh=2416d1cd3c1f
[66] (2021). *Chronicled | Automating Transactions Between Trading Partners*. [Online]. Available: https://www.chronicled.com/
[67] (2021). *Augur is the World's Most Accessible, Low-Fee, No-Limit Betting Platform*, [Online]. Available: https://augur.net/
[68] (2021). *Ternity—A Blockchain for Scalable, Secure and Decentralized Apps*. [Online]. Available: https://aeternity.com/
[69] (2021). *IBM Reveals Proof of Concept for Blockchain-Powered Internet of Things*. [Online]. Available: https://www.coindesk.com/markets/2015/01/17/ibm-reveals-proof-of-concept-for-blockchain-powered-internet-of-things/
[70] (2021). *Blockchain in Insurance Market Size, Share and Global Market Forecast to 2023 | Marketsandmarkets*. [Online]. Available: https://www.marketsandmarkets.com/Market-Reports/blockchain-in-insurance-market-9714723.html
[71] (2021). *Blockchain, a Catalyst for New Approaches in Insurance: Part 1: Publications: Financial Services: Industries: PWC*. [Online]. Available: https://www.pwc.com/gx/en/industries/financial-services/publications/blockchain-a-catalyst.html
[72] (2021). *Storj—Decentralized Cloud Storage*. [Online]. Available: https://storj.io/

[73] (2021). *IPFS Powers the Distributed Web*. [Online]. Available: https://ipfs.io/#why

[74] (2021). *Bitgive |1st Bitcoin and Blockchain Non Profit Charity Organization*. [Online]. Available: https://www.bitgivefoundation.org/

[75] (2021). *Secure Decentralized Application Development—Follow My Vote*. [Online]. Available: https://followmyvote.com/

[76] (2021). *Democracy Earth*. [Online]. Available: https://democracy.earth/#/

[77] (2021). *Blockchain for Government—IBM Blockchain | IBM*. [Online]. Available: https://www.ibm.com/blockchain/industries/government

[78] (2021). *Blockchain in Government and the Public Sector | ConsenSys*. [Online]. Available: https://consensys.net/blockchain-use-cases/government-and-the-public-sector/

[79] (2021). *Blockchain in Healthcare: Top 12 Companies—The Medical Futurist*. [Online]. Available: https://medicalfuturist.com/top-12-companies-bringing-blockchain-to-healthcare/

[80] (2021). *Doc.AI—Get the Full Picture of Your Health*. [Online]. Available: https://doc.ai/

[81] (2021). *Iryo.network*. [Online]. Available: https://iryo.network/#network

[82] (2021). *Whole Genome Sequencing DNA Test | Nebula Genomics*. [Online]. Available: https://nebula.org/whole-genome-sequencing-dna-test/

[83] (2021). *Patientory Inc | Home*. [Online]. Available: https://patientory.com/

[84] (2021). *Blockchain in the Energy Sector | 2020 | Siemens Energy Global*. [Online]. Available: https://www.siemens-energy.com/global/en/news/magazine/2020/blockchain-opportunities-energy-sector.html

[85] (2021). *Acciona Uses Blockchain to Secure Its Energy Management Software*. [Online]. Available: https://www.acciona.com/updates/news/acciona-uses-blockchain-to-secure-its-energy-management-software/?_adin=02021864894

[86] J. Ahire, *Blockchain: Future?* Abu Dhabi, United Arab Emirates: Lulu, 2018.

[87] A. Ghofrani, E. Zaidan, and A. Abulibdeh, "Simulation and impact analysis of behavioral and socioeconomic dimensions of energy consumption," *Energy*, vol. 240, Feb. 2022, Art. no. 122502.

[88] A. Ghofrani, E. Zaidan, and M. Jafari, "Reshaping energy policy based on social and human dimensions: An analysis of human-building interactions among societies in transition in GCC countries," *Humanities Social Sci. Commun.*, vol. 8, no. 1, pp. 1–26, Dec. 2021.

[89] (2021). *UBS Bank, Innogy and ZF Partner to Provide Blockchain-Backed Wallets for Cars—Econotimes*. [Online]. Available: http://www.econotimes.com/UBS-bank-innogy-and-ZF-partner-to-provide-blockchain-backed-wallets-for-cars-471860

[90] (2021). *Arcade City*. [Online]. Available: https://arcade.city/

[91] P. Paganini. (2016). *Hackers Can Remotely Disable Car Alarm on Mitsubishi Outlander PHEV SUVs*. Accessed: May 7, 2020. [Online]. Available: https://securityaffairs.co/wordpress/48114/hacking/mitsubishi-outlander-phev-hacking.html/

[92] Y. Lu, "Blockchain: A survey on functions, applications and open issues," *J. Ind. Integr. Manage.*, vol. 3, no. 4, Dec. 2018, Art. no. 1850015.

[93] M. Mettler, "Blockchain technology in healthcare: The revolution starts here," in *Proc. IEEE 18th Int. Conf. e-Health Netw., Appl. Services (Healthcom)*, Sep. 2016, pp. 1–3.

[94] S. Gupta and M. Sadoghi, "Blockchain transaction processing," 2019, *arXiv:2107.11592*.

[95] H. Hou, "The application of blockchain technology in E-government in China," in *Proc. 26th Int. Conf. Comput. Commun. Netw. (ICCCN)*, Jul. 2017, pp. 1–4.

[96] S. Haber and W. S. Stornetta, "How to time-stamp a digital document," *J. Cryptol.*, vol. 3, pp. 99–111, Jan. 1991.

[97] N. Szabo. (2008). *Bit Gold*. [Online]. Available: https://unenumerated.blogspot.com/2005/12/bit-gold.html

[98] A. Luntovskyy and D. Guetter, "Cryptographic technology blockchain and its applications," in *Proc. Int. Conf. Inf. Telecommun. Technol. Radio Electron.* Cham, Switzerland: Springer, 2018, pp. 14–33.

[99] U. W. Chohan, "The double spending problem and cryptocurrencies," UNSW Bus. School, Centre Aerosp. Secur. Stud., Crit. Blockchain Res. Initiative, Int. Assoc. Hyperpolyglots, Sydney, NSW, Australia, 2017. [Online]. Available: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3090174

[100] A. Gervais, G. O. Karame, K. Wüst, V. Glykantzis, H. Ritzdorf, and S. Capkun, "On the security and performance of proof of work blockchains," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, Oct. 2016, pp. 3–16.

[101] L. Li, J. Liu, L. Cheng, S. Qiu, W. Wang, X. Zhang, and A. Zhang, "CreditCoin: A privacy-preserving blockchain-based incentive announcement network for communications of smart vehicles," *IEEE Trans. Intell. Transp. Syst.*, vol. 19, no. 7, pp. 2204–2220, Jul. 2018.

[102] F. Gao, L. Zhu, M. Shen, K. Sharif, Z. Wan, and K. Ren, "A blockchain-based privacy-preserving payment mechanism for vehicle-to-grid networks," *IEEE Netw.*, vol. 32, no. 6, pp. 184–192, Nov./Dec. 2018.

[103] H. Liu, Y. Zhang, and T. Yang, "Blockchain-enabled security in electric vehicles cloud and edge computing," *IEEE Netw.*, vol. 32, no. 3, pp. 78–83, May/Jun. 2018.

[104] E. Erdin, M. Cebe, K. Akkaya, S. Solak, E. Bulut, and S. Uluagac, "Building a private bitcoin-based payment network among electric vehicles and charging stations," in *Proc. IEEE Int. Conf. Internet Things (iThings), IEEE Green Comput. Commun. (GreenCom), IEEE Cyber, Phys. Social Comput. (CPSCom), IEEE Smart Data (SmartData)*, Jul. 2018, pp. 1609–1615.

[105] A. Lei, H. Cruickshank, Y. Cao, P. Asuquo, C. P. A. Ogah, and Z. Sun, "Blockchain-based dynamic key management for heterogeneous intelligent transportation systems," *IEEE Internet Things J.*, vol. 4, no. 6, pp. 1832–1843, Dec. 2017.

[106] M. Liu, Y. Teng, F. R. Yu, V. C. M. Leung, and M. Song, "Deep reinforcement learning based performance optimization in blockchain-enabled Internet of vehicle," in *Proc. IEEE Int. Conf. Commun. (ICC)*, May 2019, pp. 1–6.

[107] S. Jeong, N.-N. Dao, Y. Lee, C. Lee, and S. Cho, "Blockchain based billing system for electric vehicle and charging station," in *Proc. 10th Int. Conf. Ubiquitous Future Netw. (ICUFN)*, Jul. 2018, pp. 308–310.

[108] W. Hu, W. Yao, Y. Hu, and H. Li, "Collaborative optimization of distributed scheduling based on blockchain consensus mechanism considering battery-swap stations of electric vehicles," *IEEE Access*, vol. 7, pp. 137959–137967, 2019.

[109] M. Castro and B. Liskov, "Practical Byzantine fault tolerance," in *Proc. OSDI*, vol. 99, 1999, pp. 173–186.

[110] L. Lamport, R. Shostak, and M. Pease, "The byzantine generals problem," in *Proc. Concurrency, Works Leslie Lamport*, 2019, pp. 203–226.

[111] L. Zhang and Q. Li, "Research on consensus efficiency based on practical byzantine fault tolerance," in *Proc. 10th Int. Conf. Modelling, Identificat. Control (ICMIC)*, Jul. 2018, pp. 1–6.

[112] (2016). *Intel is Winning Over Blockchain Critics by Reimagining Bitcoin's DNA*. [Online]. Available: https://www.coindesk.com/intel-winning-blockchain-critics-reimaginingbitcoins-dnal

[113] (2021). *The Five Most Popular ASIC Miners for Cryptocurrency*. [Online]. Available: https://finance.yahoo.com/news/five-most-popular-asic-miners-140930780.html?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAAGfMdhlZ1m2i4KBpXC5FUmkiuMDfrsZsHjXxh_LobIAb6Se6PlxTBKBnulBoAzAAo8gPFfgwuGO6ZD8FJrr-Nt1yhWqecV1CM7eXGhq913HnXGRvmf5S7DpnIrVTPBOf_0TtTp49JMvLjQr8GJ0XLtHabtYDghSIncN_j1dMP_r4

[114] D. D. Baby, K. C. Sivarama, S. P. Cimryn, and N. Venkateswaran, "Tracking and monitoring of vehicles and a stable and secure tolltax payment methodology based on blockchain enabled cryptocurrency e-wallets," *Int. J. Eng. Adv. Technol.*, vol. 8, pp. 685–690, Apr. 2019.

[115] Z. Zhou, B. Wang, M. Dong, and K. Ota, "Secure and efficient vehicle-to-grid energy trading in cyber physical systems: Integration of blockchain and edge computing," *IEEE Trans. Syst., Man, Cybern. Syst.*, vol. 50, no. 1, pp. 43–57, Jan. 2020.

[116] Y. Wang, Z. Su, Q. Xu, and N. Zhang, "Contract based energy blockchain for secure electric vehicles charging in smart community," in *Proc. IEEE 16th Int. Conf. Dependable, Auton. Secure Comput., 16th Int. Conf. Pervasive Intell. Comput., 4th Int. Conf. Big Data Intell. Comput. Cyber Sci. Technol. Congr. (DASC/PiCom/DataCom/CyberSciTech)*, Aug. 2018, pp. 323–327.

[117] Ethereum. (2019). *Blockchain App Platform*. [Online]. Available: https://ethereum.org/

[118] *Ethereum Blockchain as a Service Now on Azure|Microsoft*, Microsoft, Piscataway, NJ, USA, 2021. [Online]. Available: https://azure.microsoft.com/es-es/blog/ethereum-blockchain-as-a-service-now-on-azure/

[119] (2021). *Hyperledger*. [Online]. Available: https://www.ibm.com/blockchain/hyperledge

[120] (2021). *Monax.io*. [Online]. Available: https://monax.io/
[121] (2021). *Hyperledger Caliper*. [Online]. Available: https://www.hyperledger.org/projects/caliper
[122] (2021). *Hyperledger Cello*. [Online]. Available: https://www.hyperledger.org/projects/cello
[123] (2021). *Hyperledger Explore*. [Online]. Available: https://www.hyperledger.org/projects/explorer
[124] D. Boughaci and O. Boughaci, "A comparative study of three blockchain emerging technologies: Bitcoin, ethereum and hyperledger," in *Proc. Int. Conf. Comput.* Cham, Switzerland: Springer, 2019, pp. 3–7.
[125] L. Mendiboure, M. A. Chalouf, and F. Krief, "Survey on blockchain-based applications in Internet of Vehicles," *Comput. Electr. Eng.*, vol. 84, Jun. 2020, Art. no. 106646.
[126] R. Taş and O. O. Tanrıöver, "Building a decentralized application on the ethereum blockchain," in *Proc. 3rd Int. Symp. Multidisciplinary Stud. Innov. Technol. (ISMSIT)*, Oct. 2019, pp. 1–4.
[127] M. Wu, T.-J. Lu, F.-Y. Ling, J. Sun, and H.-Y. Du, "Research on the architecture of Internet of Things," in *Proc. 3rd Int. Conf. Adv. Comput. Theory Eng. (ICACTE)*, vol. 5, 2010, p. V5-484.
[128] R. Khan, S. U. Khan, R. Zaheer, and S. Khan, "Future internet: The Internet of Things architecture, possible applications and key challenges," in *Proc. 10th Int. Conf. Frontiers Inf. Technol.*, Dec. 2012, pp. 257–260.
[129] L. Tuyisenge, M. Ayaida, S. Tohme, and L.-E. Afilal, "Network architectures in Internet of Vehicles (IoV): Review, protocols analysis, challenges and issues," in *Proc. Int. Conf. Internet Vehicles*. Cham, Switzerland: Springer, 2018, pp. 3–13.
[130] P. Sethi and S. R. Sarangi, "Internet of Things: Architectures, protocols, and applications," *J. Electr. Comput. Eng.*, vol. 2017, Jan. 2017, Art. no. 9324035.
[131] M. A. Pisching, M. A. O. Pessoa, F. Junqueira, D. J. dos Santos Filho, and P. E. Miyagi, "An architecture based on RAMI 4.0 to discover equipment to process operations required by products," *Comput. Ind. Eng.*, vol. 125, pp. 574–591, Nov. 2018.
[132] M. G. dos Santos, D. Ameyed, F. Petrillo, F. Jaafar, and M. Cheriet, "Internet of Things architectures: A comparative study," 2020, *arXiv:2004.12936*.
[133] (2021). *Scopus—Document Search Results*. [Online]. Available: http://bit.ly/BiovScopusresults
[134] Z. Yang, K. Yang, L. Lei, K. Zheng, and V. C. M. Leung, "Blockchain-based decentralized trust management in vehicular networks," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 1495–1505, Apr. 2019.
[135] P. K. Sharma, S. Y. Moon, and J. H. Park, "Block-VN: A distributed blockchain based vehicular network architecture in smart city," *J. Inf. Process. Syst.*, vol. 13, no. 1, pp. 184–195, 2017.
[136] Z. Yang, K. Zheng, K. Yang, and V. C. M. Leung, "A blockchain-based reputation system for data credibility assessment in vehicular networks," in *Proc. IEEE 28th Annu. Int. Symp. Pers., Indoor, Mobile Radio Commun. (PIMRC)*, Oct. 2017, pp. 1–5.
[137] N. Malik, P. Nanda, A. Arora, X. He, and D. Puthal, "Blockchain based secured identity authentication and expeditious revocation framework for vehicular networks," in *Proc. 17th IEEE Int. Conf. Trust, Secur. Privacy Comput. Commun./12th IEEE Int. Conf. Big Data Sci. Eng. (TrustCom/BigDataSE)*, Aug. 2018, pp. 674–679.
[138] M. Labrador and W. Hou, "Implementing blockchain technology in the Internet of Vehicle (IoV)," in *Proc. Int. Conf. Intell. Comput. Emerg. Appl. (ICEA)*, Aug. 2019, pp. 5–10.
[139] T. Reimers, F. Leber, and U. Lechner, "Integration of blockchain and Internet of Things in a car supply chain," in *Proc. IEEE Int. Conf. Decentralized Appl. Infrastructures (DAPPCON)*, Apr. 2019, pp. 146–151.
[140] A. Mostafa, "VANET blockchain: A general framework for detecting malicious vehicles," *J. Commun.*, vol. 14, no. 5, pp. 356–362, 2019.
[141] K. Zhang, X. Liang, R. Lu, and X. Shen, "Sybil attacks and their defenses in the Internet of Things," *IEEE Internet Things J.*, vol. 1, no. 5, pp. 372–383, Oct. 2014.
[142] G. Rathee, A. Sharma, R. Iqbal, M. Aloqaily, N. Jaglan, and R. Kumar, "A blockchain framework for securing connected and autonomous vehicles," *Sensors*, vol. 19, no. 14, p. 3165, Jul. 2019.
[143] J. Noh, S. Jeon, and S. Cho, "Distributed blockchain-based message authentication scheme for connected vehicles," *Electronics*, vol. 9, no. 1, p. 74, Jan. 2020.
[144] S. Nadeem, M. Rizwan, F. Ahmad, and J. Manzoor, "Securing cognitive radio vehicular ad hoc network with fog node based distributed blockchain cloud architecture," *Int. J. Adv. Comput. Sci. Appl.*, vol. 10, no. 1, pp. 288–295, 2019.
[145] Y. Li and B. Hu, "A consortium blockchain-enabled secure and privacy-preserving optimized charging and discharging trading scheme for electric vehicles," *IEEE Trans. Ind. Informat.*, vol. 17, no. 3, pp. 1968–1977, Mar. 2021.
[146] M. Cinque, C. Esposito, S. Russo, and O. Tamburis, "Blockchain-empowered decentralised trust management for the Internet of Vehicles security," *Comput. Electr. Eng.*, vol. 86, Sep. 2020, Art. no. 106722.
[147] R. Shrestha, R. Bajracharya, A. P. Shrestha, and S. Y. Nam, "A new type of blockchain for secure message exchange in VANET," *Digit. Commun. Netw.*, vol. 6, no. 2, pp. 177–186, May 2020.
[148] B. Chen, L. Wu, H. Wang, L. Zhou, and D. He, "A blockchain-based searchable public-key encryption with forward and backward privacy for cloud-assisted vehicular social networks," *IEEE Trans. Veh. Technol.*, vol. 69, no. 6, pp. 5813–5825, Jun. 2020.
[149] L. Nkenyereye, B. A. Tama, M. K. Shahzad, and Y.-H. Choi, "Secure and blockchain-based emergency driven message protocol for 5G enabled vehicular edge computing," *Sensors*, vol. 20, no. 1, p. 154, Dec. 2019.
[150] A. F. M. S. Akhter, M. Ahmed, A. F. M. S. Shah, A. Anwar, and A. Zengin, "A secured privacy-preserving multi-level blockchain framework for cluster based VANET," *Sustainability*, vol. 13, no. 1, p. 400, Jan. 2021.
[151] R. Gupta, A. Kumari, and S. Tanwar, "A taxonomy of blockchain envisioned edge-as-a-connected autonomous vehicles," *Trans. Emerg. Telecommun. Technol.*, vol. 32, no. 6, p. e4009, Jun. 2021.
[152] Z. Ma, J. Zhang, Y. Guo, Y. Liu, X. Liu, and W. He, "An efficient decentralized key management mechanism for VANET with blockchain," *IEEE Trans. Veh. Technol.*, vol. 69, no. 6, pp. 5836–5849, Jun. 2020.
[153] S. K. Dwivedi, R. Amin, S. Vollala, and R. Chaudhry, "Blockchain-based secured event-information sharing protocol in Internet of Vehicles for smart cities," *Comput. Electr. Eng.*, vol. 86, Sep. 2020, Art. no. 106719.
[154] Y. Li, K. Ouyang, N. Li, R. Rahmani, H. Yang, and Y. Pei, "A blockchain-assisted intelligent transportation system promoting data services with privacy protection," *Sensors*, vol. 20, no. 9, p. 2483, Apr. 2020.
[155] D. Das, S. Banerjee, and U. Biswas, "A secure vehicle theft detection framework using blockchain and smart contract," *Peer-Peer Netw. Appl.*, vol. 14, no. 2, pp. 672–686, Mar. 2021.
[156] M. S. Eddine, M. A. Ferrag, O. Friha, and L. Maglaras, "EASBF: An efficient authentication scheme over blockchain for fog computing-enabled Internet of Vehicles," *J. Inf. Secur. Appl.*, vol. 59, Jun. 2021, Art. no. 102802.
[157] J. Gao, K. O.-B. O. Agyekum, E. B. Sifah, K. N. Acheampong, Q. Xia, X. Du, M. Guizani, and H. Xia, "A blockchain-SDN-enabled Internet of Vehicles environment for fog computing and 5G networks," *IEEE Internet Things J.*, vol. 7, no. 5, pp. 4278–4291, 2019. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/8915702?casa_token=qOf7PTB1fVgAAAAA:xqIWi2FBL0oHzWc_WVb_Ei2krQm-nONfW_CXNxkXJdwLVt35xgdTUP7yumOZnQZccmD3UaT161w
[158] D. Zhang, F. R. Yu, and R. Yang, "Blockchain-based distributed software-defined vehicular networks: A dueling deep *Q*-learning approach," *IEEE Trans. Cognit. Commun. Netw.*, vol. 5, no. 4, pp. 1086–1100, Dec. 2019.
[159] S.-O. Lee, H. Jung, and B. Han, "Security assured vehicle data collection platform by blockchain: Service provider's perspective," in *Proc. 21st Int. Conf. Adv. Commun. Technol. (ICACT)*, Feb. 2019, pp. 265–268.
[160] X. Huang, C. Xu, P. Wang, and H. Liu, "LNSC: A security model for electric vehicle and charging pile management based on blockchain ecosystem," *IEEE Access*, vol. 6, pp. 13565–13574, 2018.
[161] M. Li, L. Zhu, and X. Lin, "Efficient and privacy-preserving carpooling using blockchain-assisted vehicular fog computing," *IEEE Internet Things J.*, vol. 6, no. 3, pp. 4573–4584, Jun. 2019.
[162] H. Khelifi, S. Luo, B. Nour, H. Moungla, and S. H. Ahmed, "Reputation-based blockchain for secure NDN caching in vehicular networks," in *Proc. IEEE Conf. Standards Commun. Netw. (CSCN)*, Oct. 2018, pp. 1–6.
[163] Y. Yahiatene and A. Rachedi, "Towards a blockchain and software-defined vehicular networks approaches to secure vehicular social network," in *Proc. IEEE Conf. Standards Commun. Netw. (CSCN)*, Oct. 2018, pp. 1–7.
[164] L.-A. Hîrtan and C. Dobre, "Blockchain privacy-preservation in intelligent transportation systems," in *Proc. IEEE Int. Conf. Comput. Sci. Eng. (CSE)*, Oct. 2018, pp. 177–184.
[165] J. Kang, Z. Xiong, D. Ye, D. I. Kim, J. Zhao, and D. Niyato, "Toward secure blockchain-enabled Internet of Vehicles: Optimizing consensus management using reputation and contract theory," *IEEE Trans. Veh. Technol.*, vol. 68, no. 3, pp. 2906–2920, Mar. 2019.

[166] G. Baldini, J. L. Hernández-Ramos, G. Steri, and S. N. Matheu, "Zone keys trust management in vehicular networks based on blockchain," in *Proc. Global IoT Summit (GIoTS)*, Jun. 2019, pp. 1–6.

[167] I. J. Jensen, D. F. Selvaraj, and P. Ranganathan, "Blockchain technology for networked swarms of unmanned aerial vehicles (UAVs)," in *Proc. IEEE 20th Int. Symp. World Wireless, Mobile Multimedia Netw. (WoWMoM)*, Jun. 2019, pp. 1–7.

[168] J. Qiu, D. Grace, G. Ding, J. Yao, and Q. Wu, "Blockchain-based secure spectrum trading for unmanned-aerial-vehicle-assisted cellular networks: An operator's perspective," *IEEE Internet Things J.*, vol. 7, no. 1, pp. 451–466, Jan. 2020.

[169] Y. Yao, X. Chang, J. Mišić, V. BMišić, and L. Li, "BLA: Blockchain-assisted lightweight anonymous authentication for distributed vehicular fog services," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 3775–3784, Apr. 2019.

[170] H. Chai, S. Leng, K. Zhang, and S. Mao, "Proof-of-reputation based-consortium blockchain for trust resource sharing in Internet of Vehicles," *IEEE Access*, vol. 7, pp. 175744–175757, 2019.

[171] F. Kandah, B. Huber, A. Skjellum, and A. Altarawneh, "A blockchain-based trust management approach for connected autonomous vehicles in smart cities," in *Proc. IEEE 9th Annu. Comput. Commun. Workshop Conf. (CCWC)*, Jan. 2019, pp. 0544–0549.

[172] X. L. Wang, P. Zeng, N. Patterson, F. Jiang, and R. Doss, "An improved authentication scheme for Internet of Vehicles based on blockchain technology," *IEEE Access*, vol. 7, pp. 45061–45072, 2019.

[173] J. Kang, Z. Xiong, D. Niyato, and D. I. Kim, "Incentivizing secure block verification by contract theory in blockchain-enabled vehicular networks," in *Proc. IEEE Int. Conf. Commun. (ICC)*, May 2019, pp. 1–7.

[174] M. Li, J. Weng, A. Yang, J. Liu, and X. Lin, "Toward blockchain-based fair and anonymous ad dissemination in vehicular networks," *IEEE Trans. Veh. Technol.*, vol. 68, no. 11, pp. 11248–11259, Nov. 2019.

[175] Y. Mu, F. Rezaeibagha, and K. Huang, "Policy-driven blockchain and its applications for transport systems," *IEEE Trans. Services Comput.*, vol. 13, no. 2, pp. 230–240, Apr. 2020.

[176] Q. Feng, D. He, S. Zeadally, and K. Liang, "BPAS: Blockchain-assisted privacy-preserving authentication system for vehicular ad hoc networks," *IEEE Trans. Ind. Informat.*, vol. 16, no. 6, pp. 4146–4155, Jun. 2020.

[177] X. Li, Y. Wang, P. Vijayakumar, D. He, N. Kumar, and J. Ma, "Blockchain-based mutual-healing group key distribution scheme in unmanned aerial vehicles ad-hoc network," *IEEE Trans. Veh. Technol.*, vol. 68, no. 11, pp. 11309–11322, Sep. 2019.

[178] M. Shen, J. Zhang, L. Zhu, K. Xu, and X. Tang, "Secure SVM training over vertically-partitioned datasets using consortium blockchain for vehicular social networks," *IEEE Trans. Veh. Technol.*, vol. 69, no. 6, pp. 5773–5783, Jun. 2020.

[179] S. Guo, X. Hu, Z. Zhou, X. Wang, F. Qi, and L. Gao, "Trust access authentication in vehicular network based on blockchain," *China Commun.*, vol. 16, no. 6, pp. 18–30, Jun. 2019.

[180] Q. Wang, T. Ji, Y. Guo, L. Yu, X. Chen, and P. Li, "TrafficChain: A blockchain-based secure and privacy-preserving traffic map," *IEEE Access*, vol. 8, pp. 60598–60612, 2020.

[181] C. Kaiser, M. Steger, A. Dorri, A. Festl, A. Stocker, M. Fellmann, and S. Kanhere, "Towards a privacy-preserving way of vehicle data sharing—A case for blockchain technology?" in *Proc. Int. Forum Adv. Microsyst. Automot. Appl.* Cham, Switzerland: Springer, 2018, pp. 111–122.

[182] L. Zavolokina, N. Zani, and G. Schwabe, "Why should I trust a blockchain platform? Designing for trust in the digital car dossier," in *Proc. Int. Conf. Design Sci. Res. Inf. Syst. Technol.* Cham, Switzerland: Springer, 2019, pp. 269–283.

[183] I. García-Magariño, R. Lacuesta, M. Rajarajan, and J. Lloret, "Security in networks of unmanned aerial vehicles for surveillance with an agent-based approach inspired by the principles of blockchain," *Ad Hoc Netw.*, vol. 86, pp. 72–82, Apr. 2019.

[184] R. Chaudhary, A. Jindal, G. S. Aujla, S. Aggarwal, N. Kumar, and K. K. R. Choo, "BEST: Blockchain-based secure energy trading in SDN-enabled intelligent transportation system," *Comput. Secur.*, vol. 85, pp. 288–299, Aug. 2019.

[185] I. Ali, M. Gervais, E. Ahene, and F. Li, "A blockchain-based certificateless public key signature scheme for vehicle-to-infrastructure communication in VANETs," *J. Syst. Archit.*, vol. 99, Oct. 2019, Art. no. 101636.

[186] A. Busygin, A. Konoplev, M. Kalinin, and D. Zegzhda, "Floating genesis block enhancement for blockchain based routing between connected vehicles and software-defined VANET security services," in *Proc. 11th Int. Conf. Secur. Inf. Netw.*, Sep. 2018, pp. 1–2.

[187] A. Imeri, C. Feltus, D. Khadraoui, N. Agoulmine, and D. Nicolas, "Solving the trust issues in the process of transportation of dangerous goods by using blockchain technology," in *Proc. 11th Int. Conf. Secur. Inf. Netw.*, Sep. 2018, pp. 1–2.

[188] M. Petković, V. Mihanović, and I. Vujović, "Blockchain security of autonomous maritime transport," *J. Appl. Eng. Sci.*, vol. 17, no. 3, pp. 333–337, 2019.

[189] Y. Yahiatene, A. Rachedi, M. A. Riahla, D. E. Menacer, and F. Nait-Abdesselam, "A blockchain-based framework to secure vehicular social networks," *Trans. Emerg. Telecommun. Technol.*, vol. 30, no. 8, p. e3650, Aug. 2019.

[190] N. Zhao, H. Wu, and X. Zhao, "Consortium blockchain-based secure software defined vehicular network," *Mobile Netw. Appl.*, vol. 25, no. 1, pp. 314–327, 2020.

[191] R. Shrestha and S. Y. Nam, "Regional blockchain for vehicular networks to prevent 51% attacks," *IEEE Access*, vol. 7, pp. 95021–95033, 2019.

[192] Y. Yang, D. He, H. Wang, and L. Zhou, "An efficient blockchain-based batch verification scheme for vehicular ad hoc networks," *Trans. Emerg. Telecommun. Technol.*, Dec. 2019.

[193] Y. Chen, X. Hao, W. Ren, and Y. Ren, "Traceable and authenticated key negotiations via blockchain for vehicular communications," *Mobile Inf. Syst.*, vol. 2019, pp. 1–10, Dec. 2019.

[194] R. Iqbal, T. A. Butt, M. Afzaal, and K. Salah, "Trust management in social Internet of Vehicles: Factors, challenges, blockchain, and fog solutions," *Int. J. Distrib. Sensor Netw.*, vol. 15, no. 1, pp. 1–22, 2019.

[195] M. Labrador and W. Hou, "Security mechanism for vehicle identification and transaction authentication in the Internet of Vehicle (IoV) scenario: A blockchain based model," *J. Comput. Sci.*, vol. 15, no. 2, pp. 249–257, Feb. 2019.

[196] X. Ma, C. Ge, and Z. Liu, "Blockchain-enabled privacy-preserving Internet of Vehicles: Decentralized and reputation-based network architecture," in *Proc. Int. Conf. Netw. Syst. Secur.* Cham, Switzerland: Springer, 2019, pp. 336–351.

[197] W. Ou, M. Deng, and E. Luo, "A decentralized and anonymous data transaction scheme based on blockchain and zero-knowledge proof in vehicle networking (workshop paper)," in *Proc. Int. Conf. Collaborative Comput., Netw., Appl. Worksharing*. Cham, Switzerland: Springer, 2019, pp. 712–726.

[198] L. Davi, D. Hatebur, M. Heisel, and R. Wirtz, "Combining safety and security in autonomous cars using blockchain technologies," in *Proc. Int. Conf. Comput. Saf., Rel., Secur.* Cham, Switzerland: Springer, 2019, pp. 223–234.

[199] S. Ayvaz and S. C. Cetin, "Witness of things," *Int. J. Intell. Unmanned Syst.*, vol. 7, no. 2, pp. 72–87, Apr. 2019.

[200] K. Kaur, S. Garg, G. Kaddoum, F. Gagnon, and S. H. Ahmed, "Blockchain-based lightweight authentication mechanism for vehicular fog infrastructure," in *Proc. IEEE Int. Conf. Commun. Workshops (ICC Workshops)*, May 2019, pp. 1–6.

[201] A. Saini, S. Sharma, P. Jain, V. Sharma, and A. K. Khandelwal, "A secure priority vehicle movement based on blockchain technology in connected vehicles," in *Proc. 12th Int. Conf. Secur. Inf. Netw. (SIN)*, 2019, pp. 1–8.

[202] C.-S. Shih, W.-Y. Hsieh, and C.-L. Kao, "Traceability for vehicular network real-time messaging based on blockchain technology," *J. wireless Mobile Netw. Ubiquitous Comput. Dependable Appl.*, vol. 10, no. 4, pp. 1–21, 2019.

[203] Y. Li, K. Ouyang, N. Li, R. Rahmani, H. Yang, and Y. Pei, "A blockchain-assisted intelligent transportation system promoting data services with privacy protection," *Sensors*, vol. 20, no. 9, p. 2483, Apr. 2020.

[204] L.-A. Hîrţan, C. Dobre, and H. González-Vélez, "Blockchain-based reputation for intelligent transportation systems," *Sensors*, vol. 20, no. 3, p. 791, 2020.

[205] M. S. Ferdous, M. J. M. Chowdhury, K. Biswas, N. Chowdhury, and V. Muthukkumarasamy, "Immutable autobiography of smart cars leveraging blockchain technology," *Knowl. Eng. Rev.*, vol. 35, 2020.

[206] N. Malik, P. Nanda, X. He, and R. P. Liu, "Vehicular networks with security and trust management solutions: Proposed secured message exchange via blockchain technology," *Wireless Netw.*, vol. 26, no. 6, pp. 1–20, 2020.

[207] M. Salem, "Blockchain-based authentication approach for securing transportation system," in *Proc. Int. Symp. Intell. Comput. Syst.* Cham, Switzerland: Springer, 2020, pp. 55–64.

[208] D. Wang and X. Zhang, "Secure data sharing and customized services for intelligent transportation based on a consortium blockchain," *IEEE Access*, vol. 8, pp. 56045–56059, 2020.

[209] J. Lee, J. Lee, and H. Park, "A privacy preserving blockchain-based reward solution for vehicular networks," in *Proc. IEEE Int. Conf. Consum. Electron. (ICCE)*, Jan. 2020, pp. 1–4.
[210] L. Benarous, B. Kadri, and A. Bouridane, "Blockchain-based privacy-aware pseudonym management framework for vehicular networks," *Arabian J. Sci. Eng.*, vol. 45, no. 8, pp. 1–17, 2020.
[211] S. Hafeez, M. R. Shahid, A. Sohail, S. Jabbar, M. Suleman, and M. Zafar, "Blockchain based competent consensus algorithm for secure authentication in vehicular networks," in *Proc. 3rd Int. Conf. Comput., Math. Eng. Technol. (iCoMET)*, Jan. 2020, pp. 1–6.
[212] D. B. Rawat, R. Doku, A. Adebayo, C. Bajracharya, and C. Kamhoua, "Blockchain enabled named data networking for secure vehicle-to-everything communications," *IEEE Netw.*, vol. 34, no. 5, pp. 185–189, Sep. 2020.
[213] H. Liu, P. Zhang, G. Pu, T. Yang, S. Maharjan, and Y. Zhang, "Blockchain empowered cooperative authentication with data traceability in vehicular edge computing," *IEEE Trans. Veh. Technol.*, vol. 69, no. 4, pp. 4221–4232, Apr. 2020.
[214] Y. Qian, Y. Jiang, L. Hu, M. S. Hossain, M. Alrashoud, and M. Al-Hammadi, "Blockchain-based privacy-aware content caching in cognitive Internet of Vehicles," *IEEE Netw.*, vol. 34, no. 2, pp. 46–51, Mar. 2020.
[215] A. M. Krishna and A. K. Tyagi, "Intrusion detection in intelligent transportation system and its applications using blockchain technology," in *Proc. Int. Conf. Emerg. Trends Inf. Technol. Eng. (ic-ETITE)*, Feb. 2020, pp. 1–8.
[216] L. Zhao and T. Gao, "Combination of pseudonym changing with blockchain-based data credibility for verifying accuracy of latest vehicle information in VANETs," in *Proc. Int. Conf. Innov. Mobile Internet Services Ubiquitous Comput.* Cham, Switzerland: Springer, 2021, pp. 485–493.
[217] A. M. Eltahlawy and M. A. Azer, "Using blockchain technology for the Internet of Vehicles," in *Proc. Int. Mobile, Intell., Ubiquitous Comput. Conf. (MIUCC)*, May 2021, pp. 54–61.
[218] G. Wei and Y. Ma, "Privacy protection strategy of vehicle-to-grid network based on consortium blockchain and attribute-based signature," *IOP Conf. Ser., Earth Environ. Sci.*, vol. 661, no. 1, Feb. 2021, Art. no. 012027.
[219] T. Zhou, J. Shen, Y. Ren, and S. Ji, "Threshold key management scheme for blockchain-based intelligent transportation systems," *Secur. Commun. Netw.*, vol. 2021, pp. 1–8, Sep. 2021.
[220] P. Lv, X. Zhang, J. Liu, T. Wei, and J. Xu, "Blockchain oracle-based privacy preservation and reliable identification for vehicles," in *Proc. Int. Conf. Wireless Algorithms, Syst., Appl.*, in Lecture Notes in Computer Science, vol. 12939, 2021, pp. 512–520.
[221] J. Chen, K. Li, and P. S. Yu, "Privacy-preserving deep learning model for decentralized VANETs using fully homomorphic encryption and blockchain," *IEEE Trans. Intell. Transp. Syst.*, early access, Aug. 26, 2021, doi: 10.1109/TITS.2021.3105682.
[222] V. Valaštín, K. Košt'ál, R. Bencel, and I. Kotuliak, "Blockchain based car-sharing platform," in *Proc. Int. Symp. ELMAR*, Sep. 2019, pp. 5–8.
[223] K. O.-B. O. Agyekum, Q. Xia, E. B. Sifah, S. Amofa, K. N. Acheampong, J. Gao, R. Chen, H. Xia, J. C. Gee, X. Du, and M. Guizani, "V-chain: A blockchain-based car lease platform," in *Proc. IEEE Int. Conf. Internet Things (iThings), IEEE Green Comput. Commun. (GreenCom), IEEE Cyber, Phys. Social Comput. (CPSCom), IEEE Smart Data (SmartData)*, Jul. 2018, pp. 1317–1325.
[224] G. M. Gandhi and Salvi, "Artificial intelligence integrated blockchain for training autonomous cars," in *Proc. 5th Int. Conf. Sci. Technol. Eng. Math. (ICONSTEM)*, Mar. 2019, pp. 157–161.
[225] M. Z. Masoud, Y. Jaradat, I. Jannoud, and D. Zaidan, "CarChain: A novel public blockchain-based used motor vehicle history reporting system," in *Proc. IEEE Jordan Int. Joint Conf. Electr. Eng. Inf. Technol. (JEEIT)*, Apr. 2019, pp. 683–688.
[226] B. Yin, L. Mei, Z. Jiang, and K. Wang, "Joint cloud collaboration mechanism between vehicle clouds based on blockchain," in *Proc. IEEE Int. Conf. Service-Oriented Syst. Eng. (SOSE)*, Apr. 2019, pp. 227–2275.
[227] J. Zhang, X. Huang, W. Ni, M. Wu, and R. Yu, "VeSenChain: Leveraging consortium blockchain for secure and efficient vehicular crowdsensing," in *Proc. Chin. Control Conf. (CCC)*, Jul. 2019, pp. 6339–6344.
[228] C. Chen, T. Xiao, T. Qiu, N. Lv, and Q. Pei, "Smart-contract-based economical platooning in blockchain-enabled urban Internet of Vehicles," *IEEE Trans. Ind. Informat.*, vol. 16, no. 6, pp. 4122–4133, Jun. 2020.
[229] P. G. Saranti, D. Chondrogianni, and S. Karatzas, "Autonomous vehicles and blockchain technology are shaping the future of transportation," in *Proc. 4th Conf. Sustain. Urban Mobility*. Cham, Switzerland: Springer, 2018, pp. 797–803.
[230] S. A. Bagloee, M. Tavana, G. Withers, M. Patriksson, and M. Asadi, "Tradable mobility permit with bitcoin and ethereum—A blockchain application in transportation," *Internet Things*, vol. 8, Dec. 2019, Art. no. 100103.
[231] S.-Y. Cho, N. Chen, and X. Hua, "Developing a vehicle networking platform based on blockchain technology," in *Proc. Int. Conf. Blockchain*. Cham, Switzerland: Springer, 2019, pp. 186–201Cham.
[232] C. Guo, X. Huang, C. Zhu, X. Wang, and X. Cao, "Distributed electric vehicle control model based on blockchain," *IOP Conf. Ser., Mater. Sci. Eng.*, vol. 486, no. 1, Jun. 2019, Art. no. 012046.
[233] S. S. Ramachandran, A. K. Veeraraghavan, U. Karni, and K. Sivaraman, "Development of flexible autonomous car system using machine learning and blockchain," pp. 63–72.
[234] M. N. Postorino and G. M. Sarné, "A preliminary study for an agent blockchain-based framework supporting dynamic car-pooling," in *Proc. WOA*, 2019, pp. 65–70.
[235] P. Ren, J. Xu, Y. Wang, and X. Ma, "Research and implementation of car rental alliance based on block-chain and Internet of Vehicles," *J. Appl. Sci.*, vol. 6, p. 10, 2019.
[236] Z. Abubaker, M. U. Gurmani, T. Sultana, S. Rizwan, M. Azeem, M. Z. Iftikhar, and N. Javaid, "Decentralized mechanism for hiring the smart autonomous vehicles using blockchain," in *Proc. Int. Conf. Broadband Wireless Comput., Commun. Appl.* Cham, Switzerland: Springer, 2019, pp. 733–746.
[237] Y. Fu, F. R. Yu, C. Li, T. H. Luan, and Y. Zhang, "Vehicular blockchain-based collective learning for connected and autonomous vehicles," *IEEE Wireless Commun.*, vol. 27, no. 2, pp. 197–203, Apr. 2020.
[238] V. Davydov and S. Bezzateev, "Accident detection in Internet of Vehicles using blockchain technology," in *Proc. Int. Conf. Inf. Netw. (ICOIN)*, Jan. 2020, pp. 766–771.
[239] Y. Song, Y. Fu, F. R. Yu, and L. Zhou, "Blockchain-enabled Internet of Vehicles with cooperative positioning: A deep neural network approach," *IEEE Internet Things J.*, vol. 7, no. 4, pp. 3485–3498, Apr. 2020.
[240] S. Narbayeva, T. Bakibayev, K. Abeshev, I. Makarova, K. Shubenkova, and A. Pashkevich, "Blockchain technology on the way of autonomous vehicles development," *Transp. Res. Proc.*, vol. 44, pp. 168–175, Jan. 2020.
[241] Q. Hu, S. Fong, P. Qin, J. Guo, Y. Zhang, D. Xu, Y. Chen, and A. J. Yen, "Intelligent car parking system based on blockchain processing reengineering," in *Proc. Int. Conf. e-Bus. Eng.* Cham, Switzerland: Springer, 2019, pp. 265–273.
[242] Y. Zhu, F. Du, B. Wu, and Z. Duan, "A sharing platform of emergency cars based on blockchain environment," in *Proc. Int. Conf. Frontier Comput.* Singapore: Springer, 2019, pp. 199–209.
[243] P. K. Singh, R. Singh, S. K. Nandi, K. Z. Ghafoor, D. B. Rawat, and S. Nandi, "Blockchain-based adaptive trust management in Internet of Vehicles using smart contract," *IEEE Trans. Intell. Transp. Syst.*, vol. 22, no. 6, pp. 3616–3630, Jun. 2021.
[244] Z. Shahbazi and Y.-C. Byun, "A framework of vehicular security and demand service prediction based on data analysis integrated with blockchain approach," *Sensors*, vol. 21, no. 10, p. 3314, May 2021.
[245] S. R. Maskey, S. Badsha, S. Sengupta, and I. Khalil, "ALICIA: Applied intelligence in blockchain based VANET: Accident validation as a case study," *Inf. Process. Manage.*, vol. 58, no. 3, May 2021, Art. no. 102508.
[246] D. Das, S. Banerjee, U. Ghosh, U. Biswas, and A. KashifBashir, "A decentralized vehicle anti-theft system using blockchain and smart contracts," *Peer-Peer Netw. Appl.*, vol. 14, no. 5, pp. 1–14, 2021.
[247] N. Malik, P. Nanda, X. He, and R. P. Liu, "Vehicular networks with security and trust management solutions: Proposed secured message exchange via blockchain technology," *Wireless Netw.*, vol. 26, no. 6, pp. 4207–4226, Aug. 2020.
[248] B. C. Florea and D. D. Taralunga, "Blockchain IoT for smart electric vehicles battery management," *Sustainability*, vol. 12, no. 10, p. 3984, May 2020.
[249] S. Zhou and T. Gao, "VANETs road condition warning and vehicle incentive mechanism based on blockchain," in *Proc. Int. Conf. Innov. Mobile Internet Services Ubiquitous Comput.* Cham, Switzerland: Springer, 2021, pp. 40–49.
[250] L. Campanile, M. Iacono, F. Marulli, and M. Mastroianni, "Designing a GDPR compliant blockchain-based IoV distributed information tracking system," *Inf. Process. Manage.*, vol. 58, no. 3, May 2021, Art. no. 102511.
[251] A. Bekrar, A. Ait El Cadi, R. Todosijevic, and J. Sarkis, "Digitalizing the closing-of-the-loop for supply chains: A transportation and blockchain perspective," *Sustainability*, vol. 13, no. 5, p. 2895, Mar. 2021.

[252] H. Chai, S. Leng, Y. Chen, and K. Zhang, "A hierarchical blockchain-enabled federated learning algorithm for knowledge sharing in Internet of Vehicles," *IEEE Trans. Intell. Transp. Syst.*, vol. 22, no. 7, pp. 3975–3986, Jul. 2021.

[253] C. Zhang, W. Li, Y. Luo, and Y. Hu, "AIT: An AI-enabled trust management system for vehicular networks using blockchain technology," *IEEE Internet Things J.*, vol. 8, no. 5, pp. 3157–3169, Mar. 2021.

[254] H. Chauhan, D. Kumar, D. Gupta, S. Gupta, and V. Verma, "Blockchain and IoT based vehicle tracking system for industry 4.0 applications," *IOP Conf. Ser., Mater. Sci. Eng.*, vol. 1022, no. 1, Jan. 2021, Art. no. 012051.

[255] D. Pirker, T. Fischer, H. Witschnig, and C. Steger, "Velink—A blockchain-based shared mobility platform for private and commercial vehicles utilizing ERC-721 tokens," in *Proc. IEEE 5th Int. Conf. Cryptogr., Secur. Privacy (CSP)*. Piscataway, NJ, USA: Institute of Electrical and Electronics Engineers, 2021, pp. 62–67.

[256] H. Liu, Y. Zhou, Y. Zhang, and Y. Su, "A rough set fuzzy logic algorithm for visual tracking of blockchain logistics transportation labels," *J. Intell. Fuzzy Syst.*, vol. 41, no. 4, pp. 4965–4972, Nov. 2021.

[257] J. Zhang, H. Zhao, Y. Yang, and J. Yan, "Towards transparency and trustworthy: A used-car deposit platform based on blockchain," in *Proc. IEEE 19th Int. Conf. Softw. Qual., Rel. Secur. Companion (QRS-C)*, Jul. 2019, pp. 46–50.

[258] H. Bai, C. Wu, Y. Yang, G. Xia, and Y. Jiang, "A blockchain-based traffic conditions and driving behaviors warning scheme in the Internet of Vehicles," in *Proc. IEEE 19th Int. Conf. Commun. Technol. (ICCT)*, Oct. 2019, pp. 1160–1164.

[259] V. Deshpande, L. George, and H. Badis, "SaFe: A blockchain and secure element based framework for safeguarding smart vehicles," in *Proc. 12th IFIP Wireless Mobile Netw. Conf. (WMNC)*, Sep. 2019, pp. 181–188.

[260] Y. Song, R. Yu, Y. Fu, L. Zhou, and A. Boukerche, "Multi-vehicle cooperative positioning correction framework based on vehicular blockchain," in *Proc. 9th ACM Symp. Design Anal. Intell. Veh. Netw. Appl.*, Nov. 2019, pp. 23–29.

[261] F. Knirsch, A. Unterweger, and D. Engel, "Privacy-preserving blockchain-based electric vehicle charging with dynamic tariff decisions," *Comput. Sci. Res. Develop.*, vol. 33, nos. 1–2, pp. 71–79, 2018.

[262] X. Wang and H. Shi, "Research on container transportation application based on blockchain technology," in *Proc. Asia–Pacific Conf. Intell. Med. Int. Conf. Transp. Traffic Eng. (APCIM ICTTE)*, 2018, pp. 277–281.

[263] X. Zhang and D. Wang, "Adaptive traffic signal control mechanism for intelligent transportation based on a consortium blockchain," *IEEE Access*, vol. 7, pp. 97281–97295, 2019.

[264] S. Aswathy and K. Lakshmy, "BVD—A blockchain based vehicle database system," in *Proc. Int. Symp. Secur. Comput. Commun.* Singapore: Springer, 2018, pp. 220–230Singapore.

[265] R. Ramaguru, M. Sindhu, and M. Sethumadhavan, "Blockchain for the Internet of Vehicles," in *Proc. Int. Conf. Adv. Comput. Data Sci.* Singapore: Springer, 2019, pp. 412–423.

[266] Z. Ying, M. Ma, and L. Yi, "BAVPM: Practical autonomous vehicle platoon management supported by blockchain technique," in *Proc. 4th Int. Conf. Intell. Transp. Eng. (ICITE)*, Sep. 2019, pp. 256–260.

[267] A. Islam and S. Y. Shin, "A blockchain-based secure healthcare scheme with the assistance of unmanned aerial vehicle in Internet of Things," *Comput. Electr. Eng.*, vol. 84, Jun. 2020, Art. no. 106627.

[268] S. Iqbal, A. W. Malik, A. U. Rahman, and R. M. Noor, "Blockchain-based reputation management for task offloading in micro-level vehicular fog network," *IEEE Access*, vol. 8, pp. 52968–52980, 2020.

[269] Y. Dai, D. Xu, K. Zhang, S. Maharjan, and Y. Zhang, "Deep reinforcement learning and permissioned blockchain for content caching in vehicular edge computing and networks," *IEEE Trans. Veh. Technol.*, vol. 69, no. 4, pp. 4312–4324, Apr. 2020.

[270] X. Huang, D. Ye, R. Yu, and L. Shu, "Securing parked vehicle assisted fog computing with blockchain and optimal smart contract design," *IEEE/CAA J. Autom. Sinica*, vol. 7, no. 2, pp. 426–441, Mar. 2020.

[271] V. Elagin, A. Spirkina, M. Buinevich, and A. Vladyko, "Technological aspects of blockchain application for vehicle-to-network," *Information*, vol. 11, no. 10, p. 465, Sep. 2020.

[272] C. Li, Y. Fu, F. R. Yu, T. H. Luan, and Y. Zhang, "Vehicle position correction: A vehicular blockchain networks-based GPS error sharing framework," *IEEE Trans. Intell. Transp. Syst.*, vol. 22, no. 2, pp. 898–912, Feb. 2021.

[273] J. Ma, T. Li, J. Cui, Z. Ying, and J. Cheng, "Attribute-based secure announcement sharing among vehicles using blockchain," *IEEE Internet Things J.*, vol. 8, no. 13, pp. 10873–10883, Jul. 2021.

[274] M. Kim, J. Lee, K. Park, Y. Park, K. H. Park, and Y. Park, "Design of secure decentralized car-sharing system using blockchain," *IEEE Access*, vol. 9, pp. 54796–54810, 2021.

[275] R. S. Kaurav, R. R. Rout, and S. Vemireddy, "Blockchain for emergency vehicle routing in healthcare services: An integrated secure and trustworthy system," in *Proc. Int. Conf. Commun. Syst. Netw. (COMSNETS)*. Piscataway, NJ, USA: Institute of Electrical and Electronics Engineers, 2021, pp. 623–628.

[276] J. H. S and A. S, "Reputation management in vehicular network using blockchain," *Peer-to-Peer Netw. Appl.*, Nov. 2021.

[277] M. Abdel-Basset, N. Moustafa, H. Hawash, I. Razzak, K. M. Sallam, and O. M. Elkomy, "Federated intrusion detection in blockchain-based smart transportation systems," *IEEE Trans. Intell. Transp. Syst.*, early access, Oct. 26, 2021, doi: 10.1109/TITS.2021.3119968.

[278] R. Kumar, P. Kumar, R. Tripathi, G. P. Gupta, N. Kumar, and M. M. Hassan, "A privacy-preserving-based secure framework using blockchain-enabled deep-learning in cooperative intelligent transport system," *IEEE Trans. Intell. Transp. Syst.*, early access, Aug. 3, 2021, doi: 10.1109/TITS.2021.3098636.

[279] X. Chen and X. Zhang, "Secure electricity trading and incentive contract model for electric vehicle based on energy blockchain," *IEEE Access*, vol. 7, pp. 178763–178778, 2019.

[280] Z. Zhou, L. Tan, and G. Xu, "Blockchain and edge computing based vehicle-to-grid energy trading in energy internet," in *Proc. 2nd IEEE Conf. Energy Internet Energy Syst. Integr. (EI)*, Oct. 2018, pp. 1–5.

[281] Z. Zhou, B. Wang, Y. Guo, and Y. Zhang, "Blockchain and computational intelligence inspired incentive-compatible demand response in internet of electric vehicles," *IEEE Trans. Emerg. Topics Comput. Intell.*, vol. 3, no. 3, pp. 205–216, May 2019.

[282] M. Pustisek, A. Kos, and U. Sedlar, "Blockchain based autonomous selection of electric vehicle charging station," in *Proc. Int. Conf. Identificat., Inf. Knowl. Internet Things (IIKI)*, Oct. 2016, pp. 217–222.

[283] C. Gorenflo, L. Golab, and S. Keshav, "Mitigating trust issues in electric vehicle charging using a blockchain," in *Proc. 10th ACM Int. Conf. Future Energy Syst.*, Jun. 2019, pp. 160–164.

[284] H. Sun, S. Hua, E. Zhou, B. Pi, J. Sun, and K. Yamashita, "Using ethereum blockchain in Internet of Things: A solution for electric vehicle battery refueling," in *Blockchain—ICBC 2018*, S. Chen, H. Wang, and L.-J. Zhang, Eds. Cham, Switzerland: Springer, 2018, pp. 3–17.

[285] C. Liu, K. K. Chai, E. T. Lau, and Y. Chen, "Blockchain based energy trading model for electric vehicle charging schemes," in *Smart Grid and Innovative Frontiers in Telecommunications*, P. H. J. Chong, B.-C. Seet, M. Chai, S. U. Rehman, Eds., Cham, Switzerland: Springer, 2018, pp. 64–72.

[286] S. Thakur and G. J. Breslin, "Electric vehicle charging queue management with blockchain," in *Internet of Vehicles. Technologies and Services Towards Smart City*, A. M. J. Skulimowski, Z. Sheng, S. Khemiri-Kallel, C. Cérin, and C.-H. Hsu, Eds. Cham, Switzerland: Springer, 2018, pp. 249–264.

[287] A. R. Pedrosa and G. Pau, "ChargeltUp: On blockchain-based technologies for autonomous vehicles," in *Proc. 1st Workshop Cryptocurrencies Blockchains Distrib. Syst.*, 2018, pp. 87–92.

[288] F. C. Silva, M. A. Ahmed, J. M. Martínez, and Y.-C. Kim, "Design and implementation of a blockchain-based energy trading platform for electric vehicles in smart campus parking lots," *Energies*, vol. 12, no. 24, p. 4814, Dec. 2019.

[289] Z. Fu, P. Dong, and Y. Ju, "An intelligent electric vehicle charging system for new energy companies based on consortium blockchain," *J. Cleaner Prod.*, vol. 261, Jul. 2020, Art. no. 121219.

[290] Y. Li and B. Hu, "An iterative two-layer optimization charging and discharging trading scheme for electric vehicle using consortium blockchain," *IEEE Trans. Smart Grid*, vol. 11, no. 3, pp. 2627–2637, May 2020.

[291] M. M. Islam, M. Shahjalal, M. K. Hasan, and Y. M. Jang, "Blockchain-based energy transaction model for electric vehicles in V2G network," in *Proc. Int. Conf. Artif. Intell. Inf. Commun. (ICAIIC)*, Feb. 2020, pp. 628–630.

[292] I. A. Umoren, S. S. A. Jaffary, M. Z. Shakir, K. Katzis, and H. Ahmadi, "Blockchain-based energy trading in electric-vehicle-enabled microgrids," *IEEE Consum. Electron. Mag.*, vol. 9, no. 6, pp. 66–71, Nov. 2020.

[293] C. Liu, K. K. Chai, and X. Zhang, "Adaptive blockchain-based electric vehicle participation scheme in smart grid platform," *IEEE Access*, vol. 6, pp. 25657–25665, 2018.

[294] Z. Fu, P. Dong, and Y. Ju, "An intelligent electric vehicle charging system for new energy companies based on consortium blockchain," *J. Cleaner Prod.*, vol. 261, Jul. 2020, Art. no. 121219.

[295] M. U. Javed, N. Javaid, A. Aldegheishem, N. Alrajeh, M. Tahir, and M. Ramzan, "Scheduling charging of electric vehicles in a secured manner by emphasizing cost minimization using blockchain technology and IPFS," *Sustainability*, vol. 12, no. 12, p. 5151, Jun. 2020.
[296] G. Sun, M. Dai, F. Zhang, H. Yu, X. Du, and M. Guizani, "Blockchain-enhanced high-confidence energy sharing in internet of electric vehicles," *IEEE Internet Things J.*, vol. 7, no. 9, pp. 7868–7882, 2020.
[297] I. A. Umoren, S. S. A. Jaffary, M. Z. Shakir, K. Katzis, and H. Ahmadi, "Blockchain-based energy trading in electric-vehicle-enabled microgrids," *IEEE Consum. Electron. Mag.*, vol. 9, no. 6, pp. 66–71, Nov. 2020.
[298] Y. Long, Y. Chen, W. Ren, H. Dou, and N. N. Xiong, "DePET: A decentralized privacy-preserving energy trading scheme for vehicular energy network via blockchain and K-anonymity," *IEEE Access*, vol. 8, pp. 192587–192596, 2020.
[299] Z. Huang, Z. Li, C. S. Lai, Z. Zhao, X. Wu, X. Li, N. Tong, and L. L. Lai, "A novel power market mechanism based on blockchain for electric vehicle charging stations," *Electronics*, vol. 10, no. 3, p. 307, Jan. 2021.
[300] A. Sadiq, M. U. Javed, R. Khalid, A. Almogren, M. Shafiq, and N. Javaid, "Blockchain based data and energy trading in internet of electric vehicles," *IEEE Access*, vol. 9, pp. 7000–7020, 2021.
[301] K. Sukkrajang, R. Duangsoithong, and K. Chalermyannont, "Trade distance and price model for electric vehicle charging using blockchain-based technology," in *Proc. 18th Int. Conf. Elect. Eng./Electron., Comput., Telecommun. Inf. Technol. (ECTI-CON)*, 2021, pp. 964–967.
[302] B. Mika and A. Goudz, "Blockchain-technology in the energy industry: Blockchain as a driver of the energy revolution? With focus on the situation in Germany," *Energy Syst.*, vol. 12, no. 2, pp. 285–355, May 2021.
[303] J. C. Ferreira, C. Ferreira da Silva, and J. P. Martins, "Roaming service for electric vehicle charging using blockchain-based digital identity," *Energies*, vol. 14, no. 6, p. 1686, Mar. 2021.
[304] S. N. Gowda, B. A. Eraqi, H. Nazaripouya, and R. Gadh, "Assessment and tracking electric vehicle battery degradation cost using blockchain," in *Proc. IEEE Power Energy Soc. Innov. Smart Grid Technol. Conf. (ISGT)*, Feb. 2021, pp. 1–5.
[305] L. P. Qian, Y. Wu, X. Xu, B. Ji, Z. Shi, and W. Jia, "Distributed charging-record management for electric vehicle networks via blockchain," *IEEE Internet Things J.*, vol. 8, no. 4, pp. 2150–2162, Feb. 2021.
[306] M. Baza, R. Amer, A. Rasheed, G. Srivastava, M. Mahmoud, and W. Alasmary, "A blockchain-based energy trading scheme for electric vehicles," Inst. Elect. Electron. Eng., Piscataway, NJ, USA, 2021, pp. 1–7.
[307] H. N. Abishu, A. M. Seid, Y. H. Yacob, T. Ayall, G. Sun, and G. Liu, "Consensus mechanism for blockchain-enabled vehicle-to-vehicle energy trading in the internet of electric vehicles," *IEEE Trans. Veh. Technol.*, vol. 71, no. 1, pp. 946–960, Jan. 2022.
[308] M. U. Javed, N. Javaid, M. W. Malik, M. Akbar, O. Samuel, A. S. Yahaya, and J. B. Othman, "Blockchain based secure, efficient and coordinated energy trading and data sharing between electric vehicles," *Cluster Comput.*, pp. 1–29, 2021. [Online]. Available: https://link.springer.com/article/10.1007/s10586-021-03435-9#citeas
[309] H. Hata and S. Teramoto, "A payment system for regional transport services by blockchain with IC card and the application for transaction settlement of local economy," *IEEJ Trans. Electron., Inf. Syst.*, vol. 141, no. 8, pp. 903–908, 2021.
[310] J. Zhao, C. He, C. Peng, and X. Zhang, "Blockchain for effective renewable energy management in the intelligent transportation system," *J. Interconnection Netw.*, Jul. 2021, Art. no. 2141009.
[311] N. Zhao and H. Wu, "Blockchain combined with smart contract to keep safety energy trading for autonomous vehicles," in *Proc. IEEE 89th Veh. Technol. Conf. (VTC-Spring)*, Apr. 2019, pp. 1–5.
[312] S. Xu, X. Chen, and Y. He, "EVchain: An anonymous blockchain-based system for charging-connected electric vehicles," *Tsinghua Sci. Technol.*, vol. 26, no. 6, pp. 845–856, Dec. 2021.
[313] M. Aloqaily, I. A. Ridhawi, and M. Guizani, "Energy-aware blockchain and federated learning-supported vehicular networks," *IEEE Trans. Intell. Transp. Syst.*, early access, Aug. 17, 2022, doi: 10.1109/TITS.2021.3103645.
[314] U. Asfia, V. Kamuni, A. Sheikh, S. Wagh, and D. Patel, "Energy trading of electric vehicles using blockchain and smart contracts," in *Proc. 18th Eur. Control Conf. (ECC)*, Jun. 2019, pp. 3958–3963.
[315] Z. Su, Y. Wang, Q. Xu, M. Fei, Y.-C. Tian, and N. Zhang, "A secure charging scheme for electric vehicles with smart communities in energy blockchain," *IEEE Internet Things J.*, vol. 6, no. 3, pp. 4601–4613, Jun. 2019.
[316] H. Liu, Y. Zhang, S. Zheng, and Y. Li, "Electric vehicle power trading mechanism based on blockchain and smart contract in V2G network," *IEEE Access*, vol. 7, pp. 160546–160558, 2019.
[317] Y. Wang, Z. Su, and N. Zhang, "BSIS: Blockchain-based secure incentive scheme for energy delivery in vehicular energy network," *IEEE Trans. Ind. Informat.*, vol. 15, no. 6, pp. 3620–3631, Jun. 2019.
[318] M. Kim, K. Park, S. Yu, J. Lee, Y. Park, S.-W. Lee, and B. Chung, "A secure charging system for electric vehicles based on blockchain," *Sensors*, vol. 19, no. 13, p. 3028, Jul. 2019.
[319] X. Chen, T. Zhang, W. Ye, Z. Wang, and H. H.-C. Iu, "Blockchain-based electric vehicle incentive system for renewable energy consumption," *IEEE Trans. Circuits Syst. II, Exp. Briefs*, vol. 68, no. 1, pp. 396–400, Jan. 2021.
[320] S. Velliangiri, G. K. L. Kumar, and P. Karthikeyan, "Unsupervised blockchain for safeguarding confidential information in vehicle assets transfer," in *Proc. 6th Int. Conf. Adv. Comput. Commun. Syst. (ICACCS)*, Mar. 2020, pp. 44–49.
[321] M. Cebe, E. Erdin, K. Akkaya, H. Aksu, and S. Uluagac, "Block4Forensic: An integrated lightweight blockchain framework for forensics applications of connected vehicles," *IEEE Commun. Mag.*, vol. 56, no. 10, pp. 50–57, Oct. 2018.
[322] K. L. Brousmiche, T. Heno, C. Poulain, A. Dalmieres, and E. Ben Hamida, "Digitizing, securing and sharing vehicles life-cycle over a consortium blockchain: Lessons learned," in *Proc. 9th IFIP Int. Conf. New Technol., Mobility Secur. (NTMS)*, Feb. 2018, pp. 1–5.
[323] T. G. Jiang, H. Fang, and H. Wang, "Blockchain-based Internet of Vehicles: Distributed network architecture and performance analysis," *IEEE Internet Things J.*, vol. 6, no. 3, pp. 4640–4649, Jun. 2019.
[324] K. Leo Brousmiche, A. Durand, T. Heno, C. Poulain, A. Dalmieres, and E. B. Hamida, "Hybrid cryptographic protocol for secure vehicle data sharing over a consortium blockchain," in *Proc. IEEE Int. Conf. Internet Things (iThings), IEEE Green Comput. Commun. (GreenCom), IEEE Cyber, Phys. Social Comput. (CPSCom), IEEE Smart Data (SmartData)*, Jul. 2018, pp. 1281–1286.
[325] X. Zhang and X. Chen, "Data security sharing and storage based on a consortium blockchain in a vehicular ad-hoc network," *IEEE Access*, vol. 7, pp. 58241–58254, 2019.
[326] K. Liu, W. Chen, Z. Zheng, Z. Li, and W. Liang, "A novel debt-credit mechanism for blockchain-based data-trading in Internet of Vehicles," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 9098–9111, Oct. 2019.
[327] S. Bao, Y. Cao, A. Lei, P. Asuquo, H. Cruickshank, Z. Sun, and M. Huth, "Pseudonym management through blockchain: Cost-efficient privacy preservation on intelligent transportation systems," *IEEE Access*, vol. 7, pp. 80390–80403, 2019.
[328] F. Morano, C. Ferretti, A. Leporati, P. Napoletano, and R. Schettini, "A blockchain technology for protection and probative value preservation of vehicle driver data," in *Proc. IEEE 23rd Int. Symp. Consum. Technol. (ISCT)*, Jun. 2019, pp. 167–172.
[329] R. Sharma and S. Chakraborty, "B2VDM: Blockchain based vehicular data management," in *Proc. Int. Conf. Adv. Comput., Commun. Informat. (ICACCI)*, Sep. 2018, pp. 2337–2343.
[330] F. Kandah, B. Huber, A. Altarawneh, S. Medury, and A. Skjellum, "BLAST: Blockchain-based trust management in smart cities and connected vehicles setup," in *Proc. IEEE High Perform. Extreme Comput. Conf. (HPEC)*, Sep. 2019, pp. 1–7.
[331] S. Sharma, K. K. Ghanshala, and S. Mohan, "Blockchain-based Internet of Vehicles (IoV): An efficient secure ad hoc vehicular networking architecture," in *Proc. IEEE 2nd 5G World Forum (5GWF)*, Sep. 2019, pp. 452–457.
[332] S. Bao, A. Lei, H. Cruickshank, Z. Sun, P. Asuquo, and W. Hathal, "A pseudonym certificate management scheme based on blockchain for Internet of Vehicles," in *Proc. IEEE Int. Conf. Dependable, Autonomic Secure Comput., Int. Conf. Pervasive Intell. Comput., Int. Conf. Cloud Big Data Comput., Int. Conf. Cyber Sci. Technol. Congr. (DASC/PiCom/CBDCom/CyberSciTech)*, Aug. 2019, pp. 28–35.
[333] C. Chen, J. Wu, H. Lin, W. Chen, and Z. Zheng, "A secure and efficient blockchain-based data trading approach for Internet of Vehicles," *IEEE Trans. Veh. Technol.*, vol. 68, no. 9, pp. 9110–9121, Sep. 2019.
[334] M. Baza, M. Nabil, N. Lasla, K. Fidan, M. Mahmoud, and M. Abdallah, "Blockchain-based firmware update scheme tailored for autonomous vehicles," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, Apr. 2019, pp. 1–7.
[335] H. Guo, E. Meamari, and C.-C. Shen, "Blockchain-inspired event recording system for autonomous vehicles," in *Proc. 1st IEEE Int. Conf. Hot Inf.-Centric Netw. (HotICN)*, Aug. 2018, pp. 218–222.
[336] M. Demir, O. Turetken, and A. Ferworn, "Blockchain based transparent vehicle insurance management," in *Proc. 6th Int. Conf. Softw. Defined Syst. (SDS)*, Jun. 2019, pp. 213–220.

[337] M. A. Rahman, M. M. Rashid, S. J. Barnes, and S. M. Abdullah, "A blockchain-based secure Internet of Vehicles management framework," in *Proc. U.K./China Emerg. Technol. (UCET)*, 2019, pp. 1–4.
[338] L. Zhang, M. Luo, J. Li, M. H. Au, K.-K.-R. Choo, T. Chen, and S. Tian, "Blockchain based secure data sharing system for Internet of Vehicles: A position paper," *Veh. Commun.*, vol. 16, pp. 85–93, Apr. 2019.
[339] L. Zavolokina, F. Spychiger, C. Tessone, and G. Schwabe, "Incentivizing data quality in blockchains for inter-organizational networks–learning from the digital car dossier," in *Proc. Int. Conf. Inf. Syst. (ICIS)*. San Francisco, CA, USA: University of Zurich, Dec. 2018, pp. 12–16.
[340] D. Holtkemper and S. Wieninger, "Company data in the blockchain: A juxtaposition of technological drivers and potential applications," in *Proc. Portland Int. Conf. Manage. Eng. Technol. (PICMET)*, Aug. 2018, pp. 1–7.
[341] Q. Wang, L. Zhou, Z. Tang, and G. Wang, "A consortium blockchain-based model for data sharing in internet of Vehicles," in *Proc. Int. Conf. Smart City Informatization*. Singapore: Springer, 2019, pp. 253–267.
[342] K. Shi, L. Zhu, C. Zhang, L. Xu, and F. Gao, "Blockchain-based multimedia sharing in vehicular social networks with privacy protection," *Multimedia Tools Appl.*, vol. 79, no. 11, pp. 1–21, 2020.
[343] M. U. Javed, M. Rehman, N. Javaid, A. Aldegheishem, N. Alrajeh, and M. Tahir, "Blockchain-based secure data storage for distributed vehicular networks," *Appl. Sci.*, vol. 10, no. 6, p. 2011, Mar. 2020.
[344] C. Chen, C. Wang, T. Qiu, N. Lv, and Q. Pei, "A secure content sharing scheme based on blockchain in vehicular named data networks," *IEEE Trans. Ind. Informat.*, vol. 16, no. 5, pp. 3278–3289, May 2020.
[345] Y. Lu, X. Huang, K. Zhang, S. Maharjan, and Y. Zhang, "Blockchain empowered asynchronous federated learning for secure data sharing in Internet of Vehicles," *IEEE Trans. Veh. Technol.*, vol. 69, no. 4, pp. 4298–4311, Apr. 2020.
[346] Z. Su, Y. Wang, Q. Xu, and N. Zhang, "LVBS: Lightweight vehicular blockchain for secure data sharing in disaster rescue," *IEEE Trans. Dependable Secure Comput.*, vol. 19, no. 1, pp. 19–32, Jan. 2022.
[347] M. U. Javed, M. Rehman, N. Javaid, A. Aldegheishem, N. Alrajeh, and M. Tahir, "Blockchain-based secure data storage for distributed vehicular networks," *Appl. Sci.*, vol. 10, no. 6, p. 2011, Mar. 2020.
[348] H. Li, L. Pei, D. Liao, S. Chen, M. Zhang, and D. Xu, "FADB: A fine-grained access control scheme for VANET data based on blockchain," *IEEE Access*, vol. 8, pp. 85190–85203, 2020.
[349] S. V. Sonakshi, "A blockchain-based secure car hiring system," in *Cyber Security and Digital Forensics*. Singapore: Springer, 2022, pp. 341–349.
[350] M. Haouari, M. Mhiri, M. El-Masri, and K. Al-Yafi, "A novel proof of useful work for a blockchain storing transportation transactions," *Inf. Process. Manage.*, vol. 59, no. 1, Jan. 2022, Art. no. 102749.
[351] D. Huang, Z.-Y. Tang, W.-Y. Hu, and Q.-Z. Wu, "Blockchain-based electric vehicle charging reputation management mechanism," in *Proc. Int. Conf. Artif. Intell., Big Data Algorithms (CAIBDA)*, 2021, pp. 58–61.
[352] K. Fan, Q. Pan, K. Zhang, Y. Bai, S. Sun, H. Li, and Y. Yang, "A secure and verifiable data sharing scheme based on blockchain in vehicular social networks," *IEEE Trans. Veh. Technol.*, vol. 69, no. 6, pp. 5826–5835, Jun. 2020.
[353] C. Oham, R. A. Michelin, R. Jurdak, S. S. Kanhere, and S. Jha, "B-FERL: Blockchain based framework for securing smart vehicles," *Inf. Process. Manage.*, vol. 58, no. 1, Jan. 2021, Art. no. 102426.
[354] K. Abbas, L. A. Tawalbeh, A. Rafiq, A. Muthanna, I. A. Elgendy, and A. A. A. El-Latif, "Convergence of blockchain and IoT for secure transportation systems in smart cities," *Secur. Commun. Netw.*, vol. 2021, pp. 1–13, Apr. 2021.
[355] Z. Shahbazi and Y.-C. Byun, "A framework of vehicular security and demand service prediction based on data analysis integrated with blockchain approach," *Sensors*, vol. 21, no. 10, p. 3314, May 2021.
[356] X.-J. Liu, Y.-D. Yin, W. Chen, Y.-J. Xia, J.-L. Xu, and L.-D. Han, "Secure data sharing scheme in Internet of Vehicles based on blockchain," *Zhejiang Daxue Xuebao (Gongxue Ban)/J. Zhejiang Univ., Eng. Sci.*, vol. 55, no. 5, pp. 957–965, 2021.
[357] Y. Yin, Y. Li, B. Ye, T. Liang, and Y. Li, "A blockchain-based incremental update supported data storage system for intelligent vehicles," *IEEE Trans. Veh. Technol.*, vol. 70, no. 5, pp. 4880–4893, May 2021.
[358] S. Distefano, A. D. Giacomo, and M. Mazzara, "Trustworthiness for transportation ecosystems: The blockchain vehicle information system," *IEEE Trans. Intell. Transp. Syst.*, vol. 22, no. 4, pp. 2013–2022, Apr. 2021.
[359] J. Feng, Y. Wang, J. Wang, and F. Ren, "Blockchain-based data management and edge-assisted trusted cloaking area construction for location privacy protection in vehicular networks," *IEEE Internet Things J.*, vol. 8, no. 4, pp. 2087–2101, Feb. 2021.
[360] Y. Zou, F. Shen, F. Yan, J. Lin, and Y. Qiu, "Reputation-based regional federated learning for knowledge trading in blockchain-enhanced IoV," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*. Piscataway, NJ, USA: Institute of Electrical and Electronics Engineers, Mar. 2021, pp. 1–6.
[361] J. Wang, R. Zhu, T. Li, F. Gao, Q. Wang, and Q. Xiao, "ETC-oriented efficient and secure blockchain: Credit-based mechanism and evidence framework for vehicle management," *IEEE Trans. Veh. Technol.*, vol. 70, no. 11, pp. 11324–11337, Nov. 2021.
[362] D. Chulerttiyawong and A. Jamalipour, "A blockchain assisted vehicular pseudonym issuance and management system for conditional privacy enhancement," *IEEE Access*, vol. 9, pp. 127305–127319, 2021.
[363] Y. Ren, F. Zhu, J. Wang, P. K. Sharma, and U. Ghosh, "Novel vote scheme for decision-making feedback based on blockchain in Internet of Vehicles," *IEEE Trans. Intell. Transp. Syst.*, vol. 23, no. 2, pp. 1639–1648, Feb. 2022.
[364] B. Ghimire and D. B. Rawat, "Secure, privacy preserving and verifiable federating learning using blockchain for Internet of Vehicles," *IEEE Consum. Electron. Mag.*, early access, Jul. 29, 2021, doi: 10.1109/MCE.2021.3097705.
[365] S. K. Singh, P. K. Sharma, Y. Pan, and J. H. Park, "BIIoVT: Blockchain-based secure storage architecture for intelligent internet of vehicular things," *IEEE Consum. Electron. Mag.*, early access, Jun. 24, 2021, doi: 10.1109/MCE.2021.3089992.
[366] J. Cui, F. Ouyang, Z. Ying, L. Wei, and H. Zhong, "Secure and efficient data sharing among vehicles based on consortium blockchain," *IEEE Trans. Intell. Transp. Syst.*, early access, Jun. 16, 2021, doi: 10.1109/TITS.2021.3086976.
[367] S. Kudva, S. Badsha, S. Sengupta, H. La, I. Khalil, and M. Atiquzzaman, "A scalable blockchain based trust management in VANET routing protocol," *J. Parallel Distrib. Comput.*, vol. 152, pp. 144–156, Jun. 2021.
[368] Y. Ren, X. Li, S.-F. Sun, X. Yuan, and X. Zhang, "Privacy-preserving batch verification signature scheme based on blockchain for vehicular ad-hoc networks," *J. Inf. Secur. Appl.*, vol. 58, May 2021, Art. no. 102698.
[369] L. Sun, Q. Yang, X. Chen, and Z. Chen, "RC-chain: Reputation-based crowdsourcing blockchain for vehicular networks," *J. Netw. Comput. Appl.*, vol. 176, Feb. 2021, Art. no. 102956.
[370] L. Cui, Z. Chen, S. Yang, Z. Ming, Q. Li, Y. Zhou, S. Chen, and Q. Lu, "A blockchain-based containerized edge computing platform for the Internet of Vehicles," *IEEE Internet Things J.*, vol. 8, no. 4, pp. 2395–2408, Feb. 2021.
[371] D. Zhang, F. R. Yu, and R. Yang, "Blockchain-based multi-access edge computing for future vehicular networks: A deep compressed neural network approach," *IEEE Trans. Intell. Transp. Syst.*, early access, Oct. 8, 2021, doi: 10.1109/TITS.2021.3110591.
[372] Y. Lu, J. Zhang, Y. Qi, S. Qi, Y. Zheng, Y. Liu, H. Song, and W. Wei, "Accelerating at the edge: A storage-elastic blockchain for latency-sensitive vehicular edge computing," *IEEE Trans. Intell. Transp. Syst.*, early access, Sep. 10, 2021, doi: 10.1109/TITS.2021.3108052.
[373] Y. Hui, Y. Huang, Z. Su, T. H. Luan, N. Cheng, X. Xiao, and G. Ding, "BCC: Blockchain-based collaborative crowdsensing in autonomous vehicular networks," *IEEE Internet Things J.*, early access, Aug. 17, 2021, doi: 10.1109/JIOT.2021.3105547.
[374] M. Singh and S. Kim, "Trust bit: Reward-based intelligent vehicle commination using blockchain paper," in *Proc. IEEE 4th World Forum Internet Things (WF-IoT)*, Feb. 2018, pp. 62–67.
[375] M. Singh and S. Kim, "Introduce reward-based intelligent vehicles communication using blockchain," in *Proc. Int. SoC Design Conf. (ISOCC)*, Nov. 2017, pp. 15–16.
[376] A. A. Yusuf, D. K. Basuki, S. Sukaridhoto, Y. P. Pratama, F. B. Putra, and H. Yulianus, "ArmChain—A blockchain based sensor data communication for the vehicle as a mobile sensor network," in *Proc. Int. Electron. Symp. (IES)*, Sep. 2019, pp. 539–543.
[377] J. A. Leon Calvo and R. Mathar, "Secure blockchain-based communication scheme for connected vehicles," in *Proc. Eur. Conf. Netw. Commun. (EuCNC)*, Jun. 2018, pp. 347–351.
[378] H. Chai, S. Leng, M. Zeng, and H. Liang, "A hierarchical blockchain aided proactive caching scheme for Internet of Vehicles," in *Proc. IEEE Int. Conf. Commun. (ICC)*, May 2019, pp. 1–6.
[379] A. Kuzmin and E. Znak, "Blockchain-base structures for a secure and operate network of semi-autonomous unmanned aerial vehicles," in *Proc. IEEE Int. Conf. Service Oper. Logistics, Informat. (SOLI)*, Jul. 2018, pp. 32–37.
[380] F. Ahmad, C. A. Kerrache, F. Kurugollu, and R. Hussain, "Realization of blockchain in named data networking-based Internet-of-Vehicles," *IT Prof.*, vol. 21, no. 4, pp. 41–47, Jul. 2019.

[381] A. S. Kulathunge and H. R. O. E. Dayarathna, "Communication framework for vehicular ad-hoc networks using blockchain: Case study of metro Manila electric shuttle automation project," in *Proc. Int. Res. Conf. Smart Comput. Syst. Eng. (SCSE)*, Mar. 2019, pp. 85–90.
[382] W. Hu, Y. Hu, W. Yao, and H. Li, "A blockchain-based byzantine consensus algorithm for information authentication of the Internet of Vehicles," *IEEE Access*, vol. 7, pp. 139703–139711, 2019.
[383] A. Patel, N. Shah, T. Limbasiya, and D. Das, "VehicleChain: Blockchain-based vehicular data transmission scheme for smart city," in *Proc. IEEE Int. Conf. Syst., Man Cybern. (SMC)*, Oct. 2019, pp. 661–667.
[384] P. C. Bartolomeu and J. Ferreira, "Blockchain enabled vehicular communications: Fad or future?" in *Proc. IEEE 88th Veh. Technol. Conf. (VTC-Fall)*, Aug. 2018, pp. 1–5.
[385] B. Leiding, P. Memarmoshrefi, and D. Hogrefe, "Self-managed and blockchain-based vehicular ad-hoc networks," in *Proc. ACM Int. Joint Conf. Pervasive Ubiquitous Comput., Adjunct*, Sep. 2016, pp. 137–140.
[386] A. Gkogkidis, N. Giachoudis, G. Spathoulas, and I. Anagnostopoulos, "Implementing a blockchain infrastructure on top of vehicular ad hoc networks," in *Proc. 4th Conf. Sustain. Urban Mobility*. Cham, Switzerland: Springer, 2018, pp. 764–771.
[387] M. Singh and S. Kim, "Branch based blockchain technology in intelligent vehicle," *Comput. Netw.*, vol. 145, pp. 219–231, Nov. 2018.
[388] A. Lei, Y. Cao, S. Bao, D. Li, P. Asuquo, H. Cruickshank, and Z. Sun, "A blockchain based certificate revocation scheme for vehicular communication systems," *Future Gener. Comput. Syst.*, vol. 110, pp. 892–903, Sep. 2020.
[389] J. Wu, X. Cui, W. Hu, K. Gai, X. Liu, K. Zhang, and K. Xu, "A new sustainable interchain design on transport layer for blockchain," in *Proc. Int. Conf. Smart Blockchain*. Cham, Switzerland: Springer, 2018, pp. 12–21.
[390] A. Bonadio, F. Chiti, R. Fantacci, and V. Vespri, "An integrated framework for blockchain inspired fog communications and computing in Internet of Vehicles," *J. Ambient Intell. Humanized Comput.*, vol. 11, no. 2, pp. 755–762, Feb. 2020.
[391] M. A. Hassan, U. Habiba, U. Ghani, and M. Shoaib, "A secure message-passing framework for inter-vehicular communication using blockchain," *Int. J. Distrib. Sensor Netw.*, vol. 15, no. 2, pp. 1–12, 2019.
[392] L. Nkenyereye, B. Adhi Tama, M. K. Shahzad, and Y.-H. Choi, "Secure and blockchain-based emergency driven message protocol for 5G enabled vehicular edge computing," *Sensors*, vol. 20, no. 1, p. 154, Dec. 2019.
[393] K. M. Vidya, R. Koduri, S. Nandyala, and M. Manalikandy, "Secure vehicular communication using blockchain technology," SAE Tech. Paper 2020-01-0722, 2020.
[394] L. R. Abbade, F. M. Ribeiro, M. H. D. Silva, A. F. P. Morais, E. S. D. Morais, E. M. Lopes, A. M. Alberti, and J. J. P. C. Rodrigues, "Blockchain applied to vehicular odometers," *IEEE Netw.*, vol. 34, no. 1, pp. 62–68, Jan. 2020.
[395] P. Singh, P. Khanna, and S. Kumar, "Communication architecture for vehicular ad hoc networks, with blockchain security," in *Proc. Int. Conf. Comput., Autom. Knowl. Manage. (ICCAKM)*, Jan. 2020, pp. 68–72.
[396] A. Kumar, A. S. Yadav, and D. S. Kushwaha, "VChain: Efficient blockchain based vehicular communication protocol," in *Proc. 10th Int. Conf. Cloud Comput., Data Sci. Eng. (Confluence)*, Jan. 2020, pp. 762–768.
[397] H. Khelifi, S. Luo, B. Nour, H. Moungla, S. H. Ahmed, and M. Guizani, "A blockchain-based architecture for secure vehicular named data networks," *Comput. Electr. Eng.*, vol. 86, Sep. 2020, Art. no. 106715.
[398] Z. Zheng, J. Pan, and L. Cai, "Lightweight blockchain consensus protocols for vehicular social networks," *IEEE Trans. Veh. Technol.*, vol. 69, no. 6, pp. 5736–5748, Jun. 2020.
[399] A. F. M. S. Akhter, M. Ahmed, A. F. M. S. Shah, A. Anwar, A. S. M. Kayes, and A. Zengin, "A blockchain-based authentication protocol for cooperative vehicular ad hoc network," *Sensors*, vol. 21, no. 4, p. 1273, Feb. 2021.
[400] P. Bagga, A. K. Sutrala, A. K. Das, and P. Vijayakumar, "Blockchain-based batch authentication protocol for Internet of Vehicles," *J. Syst. Archit.*, vol. 113, Feb. 2021, Art. no. 101877.
[401] Y. Xiao, Y. Liu, and T. Li, "Edge computing and blockchain for quick fake news detection in IoV," *Sensors*, vol. 20, no. 16, p. 4360, Aug. 2020.
[402] R. Gupta, A. Kumari, and S. Tanwar, "A taxonomy of blockchain envisioned edge-as-a-connected autonomous vehicles," *Trans. Emerg. Telecommun. Technol.*, vol. 32, no. 6, p. e4009, Jun. 2021.
[403] Y. Jiang, X. Shen, and S. Zheng, "An effective data sharing scheme based on blockchain in vehicular social networks," *Electronics*, vol. 10, no. 2, pp. 1–17, 2021.
[404] H. Liao, Y. Mu, Z. Zhou, M. Sun, Z. Wang, and C. Pan, "Blockchain and learning-based secure and intelligent task offloading for vehicular fog computing," *IEEE Trans. Intell. Transp. Syst.*, vol. 22, no. 7, pp. 4051–4063, Jul. 2021.
[405] Z. Xu, W. Liang, K.-C. Li, J. Xu, and H. Jin, "A blockchain-based roadside unit-assisted authentication and key agreement protocol for Internet of Vehicles," *J. Parallel Distrib. Comput.*, vol. 149, pp. 29–39, Mar. 2021.
[406] S. Kudva, S. Badsha, S. Sengupta, I. Khalil, and A. Zomaya, "Towards secure and practical consensus for blockchain based VANET," *Inf. Sci.*, vol. 545, pp. 170–187, Feb. 2021.
[407] M. Firdaus and K.-H. Rhee, "On blockchain-enhanced secure data storage and sharing in vehicular edge computing networks," *Appl. Sci.*, vol. 11, no. 1, p. 414, Jan. 2021.
[408] M. Kamal, G. Srivastava, and M. Tariq, "Blockchain-based lightweight and secured V2V communication in the Internet of Vehicles," *IEEE Trans. Intell. Transp. Syst.*, vol. 22, no. 7, pp. 3997–4004, Jul. 2021.
[409] A. Vangala, B. Bera, S. Saha, A. K. Das, N. Kumar, and Y. Park, "Blockchain-enabled certificate-based authentication for vehicle accident detection and notification in intelligent transportation systems," *IEEE Sensors J.*, vol. 21, no. 14, pp. 15824–15838, Jul. 2021.
[410] Q. Kong, L. Su, and M. Ma, "Achieving privacy-preserving and verifiable data sharing in vehicular fog with blockchain," *IEEE Trans. Intell. Transp. Syst.*, vol. 22, no. 8, pp. 4889–4898, Aug. 2021.
[411] S. Wang, D. Ye, X. Huang, R. Yu, Y. Wang, and Y. Zhang, "Consortium blockchain for secure resource sharing in vehicular edge computing: A contract-based approach," *IEEE Trans. Netw. Sci. Eng.*, vol. 8, no. 2, pp. 1189–1201, Apr. 2021.
[412] S. Wang, S. Sun, X. Wang, Z. Ning, and J. J. P. C. Rodrigues, "Secure crowdsensing in 5G Internet of Vehicles: When deep reinforcement learning meets blockchain," *IEEE Consum. Electron. Mag.*, vol. 10, no. 5, pp. 72–81, Sep. 2021.
[413] M. Gawas, H. Patil, and S. S. Govekar, "An integrative approach for secure data sharing in vehicular edge computing using blockchain," *Peer-Peer Netw. Appl.*, vol. 14, pp. 1–19, Mar. 2021.
[414] X. Zheng, M. Li, Y. Chen, J. Guo, M. Alam, and W. Hu, "Blockchain-based secure computation offloading in vehicular networks," *IEEE Trans. Intell. Transp. Syst.*, vol. 22, no. 7, pp. 4073–4087, Jul. 2021.
[415] M. Kadadha and H. Otrok, "A blockchain-enabled relay selection for QoS-OLSR in urban VANET: A Stackelberg game model," *Ad Hoc Netw.*, vol. 117, Jun. 2021, Art. no. 102502.
[416] S. Kudva, S. Badsha, S. Sengupta, H. La, I. Khalil, and M. Atiquzzaman, "A scalable blockchain based trust management in VANET routing protocol," *J. Parallel Distrib. Comput.*, vol. 152, pp. 144–156, Jun. 2021.
[417] B. Li, R. Liang, D. Zhu, W. Chen, and Q. Lin, "Blockchain-based trust management model for location privacy preserving in VANET," *IEEE Trans. Intell. Transp. Syst.*, vol. 22, no. 6, pp. 3765–3775, Jun. 2021.
[418] E.-H. Diallo, O. Dib, N. R. Zema, and K. Al Agha, "When proof-of-work (PoW) based blockchain meets VANET environments," in *Proc. 12th Int. Conf. Inf. Commun. Syst. (ICICS)*, 2021, pp. 336–343.
[419] M. Zang, Y. Zhu, R. Lan, Y. Liu, and X. Luo, "BAVC: Efficient blockchain-based authentication scheme for vehicular secure communication," in *Proc. 13th Int. Conf. Adv. Comput. Intell. (ICACI)*, 2021, pp. 346–350.
[420] K. H. Chan, M. Pasco, and B. H. C. Cheng, "Towards a blockchain framework for autonomous vehicle system integrity," *SAE Int. J. Transp. Cybersecur. Privacy*, vol. 4, no. 1, pp. 19–38, May 2021.
[421] H. Ye and S. Park, "Reliable vehicle data storage using blockchain and IPFS," *Electronics*, vol. 10, no. 10, p. 1130, May 2021.
[422] S. Islam, S. Badsha, S. Sengupta, H. La, I. Khalil, and M. Atiquzzaman, "Blockchain-enabled intelligent vehicular edge computing," *IEEE Netw.*, vol. 35, no. 3, pp. 125–131, May 2021.
[423] Y. Zhang, J. Misic, and Z. Zheng, "Guest EditorialIntroduction to the special section on blockchain for vehicles and intelligent communications," *IEEE Trans. Veh. Technol.*, vol. 70, no. 5, pp. 3998–4000, May 2021.
[424] U. Javaid and B. Sikdar, "A secure and scalable framework for blockchain based edge computation offloading in social Internet of Vehicles," *IEEE Trans. Veh. Technol.*, vol. 70, no. 5, pp. 4022–4036, May 2021.
[425] C. Pu, "A novel blockchain-based trust management scheme for vehicular networks," in *Proc. Wireless Telecommun. Symp. (WTS)*, Apr. 2021, pp. 1–6.
[426] N. Khatri, R. Shrestha, and S. Y. Nam, "Security issues with in-vehicle networks, and enhanced countermeasures based on blockchain," *Electronics*, vol. 10, no. 8, p. 893, Apr. 2021.
[427] M. Kong, J. Zhao, X. Sun, and Y. Nie, "Secure and efficient computing resource management in blockchain-based vehicular fog computing," *China Commun.*, vol. 18, no. 4, pp. 115–125, Apr. 2021.

[428] A. Sarker, S. Byun, W. Fan, and S.-Y. Chang, "Blockchain-based root of trust management in security credential management system for vehicular communications," in *Proc. 36th Annu. ACM Symp. Appl. Comput.*, Mar. 2021, pp. 223–231.

[429] F. Ayaz, Z. Sheng, D. Tian, and Y. L. Guan, "A proof-of-quality-factor (PoQF)-based blockchain and edge computing for vehicular message dissemination," *IEEE Internet Things J.*, vol. 8, no. 4, pp. 2468–2482, Feb. 2021.

[430] D. Moussaoui, B. Kadri, M. Feham, and B. A. Bensaber, "A distributed blockchain based PKI (BCPKI) architecture to enhance privacy in VANET," in *Proc. 2nd Int. Workshop Hum.-Centric Smart Environ. Health Well-Being (IHSH)*, Feb. 2021, pp. 75–79.

[431] F. Dewanta and M. Mambo, "BPT scheme: Establishing trusted vehicular fog computing service for rural area based on blockchain approach," *IEEE Trans. Veh. Technol.*, vol. 70, no. 2, pp. 1752–1769, Feb. 2021.

[432] Q. Mei, H. Xiong, Y. Zhao, and K.-H. Yeh, "Toward blockchain-enabled IoV with edge computing: Efficient and privacy-preserving vehicular communication and dynamic updating," in *Proc. IEEE Conf. Dependable Secure Comput. (DSC)*. Piscataway, NJ, USA: Institute of Electrical and Electronics Engineers, 2021, pp. 1–8.

[433] S. More, R. Sonkamble, U. Naik, S. Phansalkar, P. More, and B. S. Saini, "Secured communication in vehicular adhoc networks (VANETs) using blockchain," *IOP Conf. Ser., Mater. Sci. Eng.*, vol. 1022, no. 1, Jan. 2021, Art. no. 012067.

[434] C. Mao, K. Xie, L. Gao, M. Wan, and S. Liu, "Design of Internet of Vehicles authentication scheme based on blockchain," *J. Phys., Conf. Ser.*, vol. 1738, no. 1, Jan. 2021, Art. no. 012097.

[435] S.-K. Kim, "Enhanced IoV security network by using blockchain governance game," *Mathematics*, vol. 9, no. 2, pp. 1–13, 2021.

[436] M. Ahmed, N. Moustafa, A. F. M. S. Akhter, I. Razzak, E. Surid, A. Anwar, A. F. M. S. Shah, and A. Zengin, "A blockchain-based emergency message transmission protocol for cooperative VANET," *IEEE Trans. Intell. Transp. Syst.*, early access, Oct. 4, 2021, doi: 10.1109/TITS.2021.3115245.

[437] Z. Zhou, M. Wang, J. Huang, S. Lin, and Z. Lv, "Blockchain in big data security for intelligent transportation with 6G," *IEEE Trans. Intell. Transp. Syst.*, early access, Sep. 3, 2021, doi: 10.1109/TITS.2021.3107011.

[438] D. Wang, L. Zhang, C. Huang, and X. Shen, "A privacy-preserving trust management system based on blockchain for vehicular networks," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*. Piscataway, NJ, USA: Institute of Electrical and Electronics Engineers, Mar. 2021, pp. 1–6.

[439] Y. Yang, L. Wei, J. Wu, C. Long, and B. Li, "A blockchain-based multi-domain authentication scheme for conditional privacy preserving in vehicular ad-hoc network," *IEEE Internet Things J.*, early access, Aug. 24, 2021, doi: 10.1109/JIOT.2021.3107443.

[440] A. Jamal, M. U. Gurmani, S. Awan, M. B. E. Sajid, S. Amjad, and N. Javaid, "Blockchain enabled secure and efficient reputation management for vehicular energy network," in *Proc. Conf. Complex, Intell., Softw. Intensive Syst.*, vol. 278, 2021, pp. 406–416.

[441] A. Jamal, S. Amjad, U. Aziz, M. U. Gurmani, S. Awan, and N. Javaid, "A privacy preserving hybrid blockchain based announcement scheme for vehicular energy network," in *Proc. Conf. Complex, Intell., Softw. Intensive Syst.*, vol. 278, 2021, pp. 142–151.

[442] V. Hassija, M. Zaid, G. Singh, A. Srivastava, and V. Saxena, "Cryptober: A blockchain-based secure and cost-optimal car rental platform," in *Proc. 12th Int. Conf. Contemp. Comput. (IC3)*, Aug. 2019, pp. 1–6.

[443] F. Jamil, O. Cheikhrouhou, H. Jamil, A. Koubaa, A. Derhab, and M. A. Ferrag, "PetroBlock: A blockchain-based payment mechanism for fueling smart vehicles," *Appl. Sci.*, vol. 11, no. 7, p. 3055, Mar. 2021.

[444] J. Wang, X. Feng, T. Xu, H. Ning, and T. Qiu, "Blockchain-based model for nondeterministic crowdsensing strategy with vehicular team cooperation," *IEEE Internet Things J.*, vol. 7, no. 9, pp. 8090–8098, Sep. 2020.

[445] Z. Ying, L. Yi, and M. Ma, "BEHT: Blockchain-based efficient highway toll paradigm for opportunistic autonomous vehicle platoon," *Wireless Commun. Mobile Comput.*, vol. 2020, pp. 1–13, Sep. 2020.

[446] J. Guo, X. Ding, and W. Wu, "Reliable traffic monitoring mechanisms based on blockchain in vehicular networks," *IEEE Trans. Rel.*, early access, Jan. 13, 2021, doi: 10.1109/TR.2020.3046556.

[447] M. Baygin, O. Yaman, N. Baygin, and M. Karakose, "A blockchain-based approach to smart cargo transportation using UHF RFID," *Expert Syst. Appl.*, vol. 188, 2022, Art. no. 116030. [Online]. Available: https://www.sciencedirect.com/science/article/abs/pii/S0957417421013762?casa_token=10kIv4CA7tEAAAAA:iPpEqxSYnyM1R5guh5a7O-spOtpXBFS_2F_HujgRkJ-lkunARgs1HLMXXf5AvVYB1IP_K0CvWyc

[448] X. Lin, J. Wu, S. Mumtaz, S. Garg, J. Li, and M. Guizani, "Blockchain-based on-demand computing resource trading in IoV-assisted smart city," *IEEE Trans. Emerg. Topics Comput.*, vol. 9, no. 3, pp. 1373–1385, 2020. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/8985250?casa_token=MycqpviqK0UAAAAA:tzXslCnroqKCGC61pcUWcK5WxBCQpWvS5lkrYBqy7kbieyoz3QefO7nS7nl-JmO_ZOz0c64YYXA

[449] "Blockchain-based privacy-preserving driver monitoring for maas in the vehicular IoT," vol. 70, no. 4, pp. 3788–3799. [Online]. Available: https://ieeexplore.ieee.org/document/9374088

[450] L. Li, X. Chang, J. Liu, J. Liu, and Z. Han, "Bit2CV: A novel bitcoin anti-fraud deposit scheme for connected vehicles," *IEEE Trans. Intell. Transp. Syst.*, vol. 22, no. 7, pp. 4181–4193, Jul. 2021.

[451] Y. Fang, Y. Zhao, Y. Yu, H. Zhu, X. Du, and M. Guizani, "Blockchain-based privacy-preserving valet parking for self-driving vehicles," *Trans. Emerg. Telecommun. Technol.*, vol. 32, no. 4, p. e4239, Apr. 2021.

[452] R. Jabbar, N. Fetais, M. Kharbeche, M. Krichen, K. Barkaoui, and A. M. Shinoy, "Blockchain for the Internet of Vehicles: How to use blockchain to secure vehicle-to-everything (V2X) communication and payment?" *IEEE Sensors J.*, vol. 21, no. 14, pp. 15807–15823, Jul. 2021.

[453] R. Jabbar, M. Krichen, M. Shinoy, M. Kharbeche, N. Fetais, and K. Barkaoui, "A model-based and resource-aware testing framework for parking system payment using blockchain," in *Proc. Int. Wireless Commun. Mobile Comput. (IWCMC)*, Jun. 2020, pp. 1252–1259.

[454] J. Pajic, J. Rivera, K. Zhang, and H.-A. Jacobsen, "EVA: Fair and auditable electric vehicle charging service using blockchain," in *Proc. 12th ACM Int. Conf. Distrib. Event-Based Syst.*, 2018, pp. 262–265. [Online]. Available: https://dl.acm.org/doi/abs/10.1145/3210284.3219776?casa_token=NS1MrdLqdbIAAAAA:7YyAauVpeV7q7ou-qbutLlm2vwosjwYjqa1loHe_toa7qwbyA2S2L1hlx_sGKtrvLsFPc4EDSaW2sQ

[455] Z. Wang, M. Ogbodo, H. Huang, C. Qiu, M. Hisada, and A. B. Abdallah, "AEBIS: AI-enabled blockchain-based electric vehicle integration system for power management in smart grid platform," *IEEE Access*, vol. 8, pp. 226409–226421, 2020.

[456] Y. Pu, T. Xiang, C. Hu, A. Alrawais, and H. Yan, "An efficient blockchain-based privacy preserving scheme for vehicular social networks," *Inf. Sci.*, vol. 540, pp. 308–324, 2020. [Online]. Available: https://www.sciencedirect.com/science/article/abs/pii/S0020025520305156?casa_token=1y66uAQnB54AAAAA:_tpY49XwR53MO6Ipj2u7h0yhLORvHKawY6iUhAuMDt5TDfQyXUR8RTKlCFCdjKGH6cQ3-OTnlK4

[457] A. Bonadio, F. Chiti, R. Fantacci, and V. Vespri, "An integrated framework for blockchain inspired fog communications and computing in Internet of Vehicles," *J. Ambient Intell. Humanized Comput.*, vol. 11, no. 2, pp. 755–762, Feb. 2020.

[458] R. Jabbar, M. Kharbeche, K. Al-Khalifa, M. Krichen, and K. Barkaoui, "Blockchain for the Internet of Vehicles: A decentralized IoT solution for vehicles communication using ethereum," *Sensors*, vol. 20, no. 14, p. 3928, Jul. 2020.

[459] R. Jabbar, M. Krichen, M. Kharbeche, N. Fetais, and K. Barkaoui, "A model-based testing framework for validating an IoT solution for blockchain-based vehicles communication," Tech. Rep., 2020.

[460] R. Jabbar, M. Krichen, M. Kharbeche, N. Fetais, and K. Barkaoui, "Un cadre de test formel pour la validation d'un système de communication inter-véhiculaire basé sur les iots et la blockchain," Tech. Rep., 2020.

[461] R. Jabbar, M. Krichen, N. Fetais, and K. Barkaoui, "Formal verification and model-based testing techniques for validating a blockchain-based healthcare records sharing system," Tech. Rep., 2020.

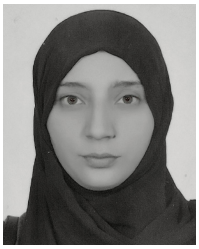
[462] R. Jabbar, K. Al-Khalifa, M. Kharbeche, W. Alhajyaseen, M. Jafari, and S. Jiang, "Applied Internet of Things IoT: Car monitoring system for modeling of road safety and traffic system in the state of qatar," in *Proc. Qatar Found. Annu. Res. Conf.* Ar-Rayyan, Qatar: Hamad bin Khalifa Univ. Press (HBKU Press), 2018, no. 3, pp. 1–2, Paper ICTPP1072.

[463] R. Jabbar, M. Shinoy, M. Kharbeche, K. Al-Khalifa, M. Krichen, and K. Barkaoui, "Urban traffic monitoring and modeling system: An IoT solution for enhancing road safety," in *Proc. Int. Conf. Internet Things, Embedded Syst. Commun. (IINTEC)*, Dec. 2019, pp. 13–18.

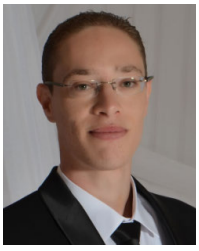
[464] R. Jabbar, K. Al-Khalifa, M. Kharbeche, W. Alhajyaseen, M. Jafari, and S. Jiang, "Real-time driver drowsiness detection for Android application using deep neural networks techniques," *Proc. Comput. Sci.*, vol. 130, pp. 400–407, Jan. 2018.

[465] R. Jabbar, M. Shinoy, M. Kharbeche, K. Al-Khalifa, M. Krichen, and K. Barkaoui, "Driver drowsiness detection model using convolutional neural networks techniques for Android application," in *Proc. IEEE Int. Conf. Inform., IoT, Enabling Technol. (ICIoT)*, Feb. 2020, pp. 237–242.
[466] L. Kenny, "The blockchain scalability problem & the race for visa-like transaction speed | by Kenny L. | towards data science," Tech. Rep., 2021.
[467] S. Biswas, K. Sharif, F. Li, B. Nour, and Y. Wang, "A scalable blockchain framework for secure transactions in IoT," *IEEE Internet Things J.*, vol. 6, no. 3, pp. 4650–4659, Jun. 2019.
[468] (2021). *Aelf—A Multi-Chain Parallel Computing Blockchain Framework*. [Online]. Available: https://aelf.io/gridcn/aelf_whitepaper_EN.pdf?v=1.6
[469] J. Kan, S. Chen, and X. Huang, "Improve blockchain performance using graph data structure and parallel mining," in *Proc. 1st IEEE Int. Conf. Hot Information-Centric Netw. (HotICN)*, Aug. 2018, pp. 173–178.
[470] *Graphchain: A Framework for On-Chain Data Management for Ontochain | Ontochain*, 2021.
[471] N. Van Toan, U. Park, and G. Ryu, "RCANE: Semi-centralized network of parallel blockchain and APoS," in *Proc. IEEE 24th Int. Conf. Parallel Distrib. Syst. (ICPADS)*, Dec. 2018, pp. 1–6.
[472] M. Fitzi, P. Gazi, A. Kiayias, and A. Russell, "Parallel chains: Improving throughput and latency of blockchain protocols via parallel composition," IACR Cryptol. ePrint Arch., Tech. Rep., 2018, p. 1119.
[473] (2020). *Smart Contract Security Verification Standard*. [Online]. Available: https://github.com/securing/SCSVS
[474] X. Fu, H. Wang, P. Shi, and H. Mi, "PoPF: A consensus algorithm for JCLedger," in *Proc. IEEE Symp. Service-Oriented Syst. Eng. (SOSE)*, Mar. 2018, pp. 204–209.
[475] N. Shibata, "Proof-of-search: Combining blockchain consensus formation with solving optimization problems," *IEEE Access*, vol. 7, pp. 172994–173006, 2019.
[476] A. M. Kudin, B. A. Kovalenko, and I. V. Shvidchenko, "Blockchain technology: Issues of analysis and synthesis," *Cybern. Syst. Anal.*, vol. 55, no. 3, pp. 488–495, May 2019.
[477] M. U. Zaman, T. Shen, and M. Min, "Proof of sincerity: A new lightweight consensus approach for mobile blockchains," in *Proc. 16th IEEE Annu. Consum. Commun. Netw. Conf. (CCNC)*. Piscataway, NJ, USA: IEEE, 2019, pp. 1–4.
[478] F. Bravo-Marquez, S. Reeves, and M. Ugarte, "Proof-of-learning: A blockchain consensus mechanism based on machine learning competitions," in *Proc. IEEE Int. Conf. Decentralized Appl. Infrastructures (DAPPCON)*, Apr. 2019, pp. 119–124.
[479] C. Liu, K. K. Chai, X. Zhang, and Y. Chen, "Proof-of-benefit: A blockchain-enabled EV charging scheme," in *Proc. IEEE 89th Veh. Technol. Conf. (VTC-Spring)*, Apr. 2019, pp. 1–6.
[480] S. Masseport, B. Darties, R. Giroudeau, and J. Lartigau, "Proof of experience: Empowering proof of work protocol with miner previous work," in *Proc. 2nd Conf. Blockchain Res. Appl. Innov. Netw. Services (BRAINS)*, Sep. 2020, pp. 57–58.
[481] F. Bizzaro, M. Conti, and M. S. Pini, "Proof of evolution: Leveraging blockchain mining for a cooperative execution of genetic algorithms," in *Proc. IEEE Int. Conf. Blockchain (Blockchain)*, Nov. 2020, pp. 450–455.
[482] S. Sayeed and H. Marco-Gisbert, "Proof of adjourn (PoAj): A novel approach to mitigate blockchain attacks," *Appl. Sci.*, vol. 10, no. 18, p. 6607, Sep. 2020.
[483] A. Ben Said and A. Erradi, "A probabilistic approach for maximizing travel journey WiFi coverage using mobile crowdsourced services," *IEEE Access*, vol. 7, pp. 82297–82307, 2019.
[484] M. Abdelhedi, R. Jabbar, T. Mnif, and C. Abbes, "Prediction of uniaxial compressive strength of carbonate rocks and cement mortar using artificial neural network and multiple linear regressions," *Acta Geodynamica Geromaterialia*, vol. 17, no. 3, pp. 367–378, 2020.
[485] S. Ayadi, A. B. Said, R. Jabbar, C. Aloulou, A. Chabbouh, and A. B. Achballah, "Dairy cow rumination detection: A deep learning approach," in *Proc. Int. Workshop Distrib. Comput. Emerg. Smart Netw.* Cham, Switzerland: Springer, 2020, pp. 123–139.
[486] E. Baccour, F. Haouari, A. Erbad, A. Mohamed, K. Bilal, M. Guizani, and M. Hamdi, "An intelligent resource reservation for crowdsourced live video streaming applications in geo-distributed cloud environment," *IEEE Syst. J.*, early access, Jun. 2, 2021, doi: 10.1109/JSYST.2021.3077707.
[487] R. Hamdi, E. Baccour, A. Erbad, M. Qaraqe, and M. Hamdi, "LoRa-RL: Deep reinforcement learning for resource management in hybrid energy LoRa wireless networks," *IEEE Internet Things J.*, early access, Sep. 8, 2021, doi: 10.1109/JIOT.2021.3110996.
[488] T. Wang, S. C. Liew, and S. Zhang, "When blockchain meets AI: Optimal mining strategy achieved by machine learning," *Int. J. Intell. Syst.*, vol. 36, no. 5, pp. 2183–2207, May 2021.
[489] Z. Du, C. Wu, T. Yoshinaga, K.-L.-A. Yau, Y. Ji, and J. Li, "Federated learning for vehicular Internet of Things: Recent advances and open issues," *IEEE Open J. Comput. Soc.*, vol. 1, pp. 45–61, 2020.
[490] C. Ma, J. Li, M. Ding, L. Shi, T. Wang, Z. Han, and H. V. Poor, "When federated learning meets blockchain: A new distributed learning paradigm," 2020, *arXiv:2009.09338*.
[491] S. Otoum, I. Al Ridhawi, and H. T. Mouftah, "Blockchain-supported federated learning for trustworthy vehicular networks," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2020, pp. 1–6.
[492] M. Z. Ge, H. Bangui, and B. Buhnova, "Big data for Internet of Things: A survey," *Future Gener. Comput. Syst.*, vol. 87, pp. 601–614, Oct. 2018.
[493] O. Nasraoui and C.-E. B. N'Cir, *Clustering Methods for Big Data Analytics: Techniques, Toolboxes and Applications*. Springer, 2019, p. 192.
[494] E. Karafiloski and A. Mishev, "Blockchain solutions for big data challenges: A literature review," in *Proc. IEEE 17th Int. Conf. Smart Technol. (EUROCON)*, Jul. 2017, pp. 763–768.
[495] Z. Wang, Y. Tian, and J. Zhu, "Data sharing and tracing scheme based on blockchain," in *Proc. 8th Int. Conf. Logistics, Informat. Service Sci. (LISS)*, Aug. 2018, pp. 1–6.
[496] L. Yue, H. Junqin, Q. Shengzhi, and W. Ruijin, "Big data model of security sharing based on blockchain," in *Proc. 3rd Int. Conf. Big Data Comput. Commun. (BIGCOM)*, Aug. 2017, pp. 117–121.
[497] F. Grée, V. Laznikova, B. Kim, G. Garcia, T. Kigezi, and B. Gao, "Cloud-based big data platform for vehicle-to-grid (V2G)," *World Electric Vehicle J.*, vol. 11, no. 2, p. 30, Mar. 2020.
[498] D. Fang, Y. Qian, and R. Q. Hu, "Security for 5G mobile wireless networks," *IEEE Access*, vol. 6, pp. 4850–4874, 2017.
[499] D. Fang and Y. Qian, "5G wireless security and privacy: Architecture and flexible mechanisms," *IEEE Veh. Technol. Mag.*, vol. 15, no. 2, pp. 58–64, Jun. 2020.
[500] A. M. Alwakeel, A. K. Alnaim, and E. B. Fernandez, "A survey of network function virtualization security," in *Proc. SoutheastCon*, Apr. 2018, pp. 1–8.
[501] H. Wang, D. He, J. Yu, N. N. Xiong, and B. Wu, "RDIC: A blockchain-based remote data integrity checking scheme for IoT in 5G networks," *J. Parallel Distrib. Comput.*, vol. 152, pp. 1–10, Jun. 2021.
[502] G. S. Aujla, M. Singh, A. Bose, N. Kumar, G. Han, and R. Buyya, "BlockSDN: Blockchain-as-a-service for software defined networking in smart city applications," *IEEE Netw.*, vol. 34, no. 2, pp. 83–91, Mar. 2020.
[503] R. Rosa and C. E. Rothenberg, "Blockchain-based decentralized applications for multiple administrative domain networking," *IEEE Commun. Standards Mag.*, vol. 2, no. 3, pp. 29–37, Oct. 2018.
[504] S. Zhang, "An overview of network slicing for 5G," *IEEE Wireless Commun.*, vol. 26, no. 3, pp. 111–117, Jun. 2019.
[505] B. Nour, A. Ksentini, N. Herbaut, P. A. Frangoudis, and H. Moungla, "A blockchain-based network slice broker for 5G services," *IEEE Netw. Lett.*, vol. 1, no. 3, pp. 99–102, Sep. 2019.
[506] V. A. Siris, D. Dimopoulos, N. Fotiou, S. Voulgaris, and G. C. Polyzos, "Trusted D2D-based IoT resource access using smart contracts," in *Proc. IEEE 20th Int. Symp. World Wireless, Mobile Multimedia Netw. (WoWMoM)*, Jun. 2019, pp. 1–9.
[507] H. Cui, Z. Chen, N. Liu, and B. Xia, "Blockchain-driven contents sharing strategy for wireless cache-enabled D2D networks," in *Proc. IEEE Int. Conf. Commun. Workshops (ICC Workshops)*, May 2019, pp. 1–5.
[508] L. Xie, Y. Ding, H. Yang, and X. Wang, "Blockchain-based secure and trustworthy Internet of Things in SDN-enabled 5G-VANETs," *IEEE Access*, vol. 7, pp. 56656–56666, 2019.
[509] V. Adat, I. Politis, C. Tselios, P. Galiotos, and S. Kotsopoulos, "On blockchain enhanced secure network coding for 5G deployments," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2018, pp. 1–7.
[510] V. Ortega, F. Bouchmal, and J. F. Monserrat, "Trusted 5G vehicular networks: Blockchains and content-centric networking," *IEEE Veh. Technol. Mag.*, vol. 13, no. 2, pp. 121–127, Jun. 2018.
[511] S. Sharma, R. Miller, and A. Francini, "A cloud-native approach to 5G network slicing," *IEEE Commun. Mag.*, vol. 55, no. 8, pp. 120–127, Aug. 2017.

RATEB JABBAR received the Ph.D. degree in computer Science from Hautes Écoles Sorbonne Arts et Métiers (HESAM) University, Paris, France, in 2021. He worked as a Senior Software Engineer for ten years specialist in web, cloud, machine learning, and blockchain technologies. He is a Postdoctoral Fellow with the Department of Computer Science and Engineering, Qatar University. He is a Microsoft Certified Professional and a Microsoft Certified Technology Specialist in developing ASP.NET MVC 4 web applications and Microsoft Azure cloud service and web services.



EYA DHIB received the Ph.D. degree in information and communication technology from the Higher School of Communication of Tunis (Sup'Com), University of Carthage, in 2018. She is a Postdoctoral Fellow at Sup'Com. Her research interests include cloud computing, cloud gaming, and machine learning.



AHMED BEN SAID received the Ph.D. degree in computer Science from the University of Burgundy, France, in 2015. He was a Research Assistant with Qatar University on several projects, including the simulation of a surgical cutting operation using 3-D modeling, the usage of multispectral image for face recognition, and the development of reliable mHealth systems for remote patient diagnosis. He currently holds a postdoctoral position at Qatar University. His research interests include machine learning and computer vision. He is also interested in crowd-sourced mobile applications and mobile health systems.

MOEZ KRICHEN (Member, IEEE) received the Ph.D. degree in computer science from Joseph Fourier University, Grenoble, France, in 2007, and the HDR (Ability to Conduct Researches) degree in computer science from the University of Sfax, Sfax, Tunisia, in 2018. He is currently an Assistant Professor at the National School of Engineers of Sfax and a member of the Research Laboratory on Development and Control of Distributed Applications (REDCAD), Sfax. His main research interests include model-based conformance, load, and security testing methodologies for real-time, distributed, and dynamically adaptable systems. Moreover, he works on applying formal methods to several modern technologies like smart cities, the Internet of Things (IoT), smart vehicles, drones, and healthcare systems. Currently, he is also working on formal aspects related to deep learning, data mining, blockchain, smart contracts, and optimization.

NOORA FETAIS (Senior Member, IEEE) is an Assistant Professor with the Department of Computer Science and Engineering, Qatar University. Her research interests include visualization for cybersecurity, and emerging technologies. She is a Senior Member of ACM.

ESMAT ZAIDAN received the bachelor's degree in civil engineering, the master's degree in architectural planning and cities design, the master's degree in applied environmental studies in local economic development, and the Ph.D. degree in geography and environmental management from the University of Waterloo, Canada. She has worked with the World Bank for more than eight years in many development projects in Palestine. She worked as an Assistant Professor of urban planning with United Arab Emirates University, and as a Lecturer of international development with the University of Waterloo. She currently works as an Associate Professor of planning and development with Qatar University. She has worked closely with many international development organizations, planners, and community members when conducting sustainability-oriented research in Toronto, Dubai, Abu Dhabi, and Doha. She has published two books, eight book-chapters, and a wider range of articles (more than 22) in top-tier journals (ISI-Scopus) by Elsevier, Sage, Routledge, and Taylor & Francis. She has conference papers in more than ten countries. Her research interests include smart urban planning and development, sustainable development planning and policy, urban sustainability and adaptation context for planning policies, technological and human factors of the transition to sustainability, implications of sustainable transportation systems on sustainable development, and sustainability of tourism development.

KAMEL BARKAOUI is a Full Professor at the Conservatoire National des Arts et Métiers (Le Cnam), Paris. His research interests include formal methods for verification, control, and performance evaluation of concurrent and distributed systems. He received the Outstanding Paper Award at the IEEE Int. Conf. on System Man and Cybernetics (Vancouver 1995) and has been a recipient of the "Prime d'excellence scientifique," since 1998. He is the SC Chair of the International Conference on Verification and Evaluation of Computer and Communication Systems (VECoS). He was the General Co-Chair of the 18th International Symposium on Formal Methods (FM 2012) and the 13th Colloquium on Modelling of Reactive Systems (MSR 2021), and the General Chair of 35th International Conference on Application and Theory of Petri Nets and Concurrency (Petri Nets 2014) and the 14th International Conference on Application of Concurrency System Design (ACSD 2014). He leaded or participated in more than ten international research projects.