Blockchain Technology for Intelligent Transportation Systems: A Systematic Literature Review

Rateb Jabbar, Eya Dhib, Ahmed Ben Said, Moez Krichen, Noora Fetais, Esmat Zaidan, Kamel Barkaoui

IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Date of publication xxxx 00, 0000, date of current version xxxx 00, 0000.

Digital Object Identifier 10.1109/ACCESS.2021.DOI

Blockchain Technology for Intelligent Transportation Systems: A Systematic Literature Review

RATEB JABBAR[1,2], EYA DHIB[3], AHMED BEN SAID[4], MOEZ KRICHEN[5], NOORA FETAIS[4], ESMAT ZAIDAN[1] and KAMEL BARKAOUI[2]

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

Corresponding author: Rateb Jabbar (Tel.: +974-4403-4328; Fax: +974-4403-4302; E-mail: rateb.jabbar@qu.edu.qa).

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, Internet of Things, Security, Cloud and Android.

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 involving unimpaired drivers. With

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2022.3149958, IEEE Access

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, also 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 increasingly 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 most important achievement 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. Pournader 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 et al. [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

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2022.3149958, IEEE Access

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 et al. [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 imple-

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2022.3149958, IEEE Access

mentations: Bitcoin, Ethereum, and Hyperledger. In Section IV, different 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 illustrated in Figure 1 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. 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.

Figure 1: Key concepts of Blockchain

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

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

[30].

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

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2022.3149958, IEEE Access

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 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

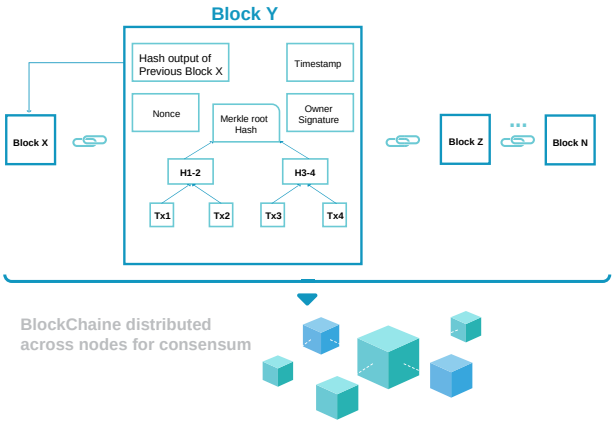


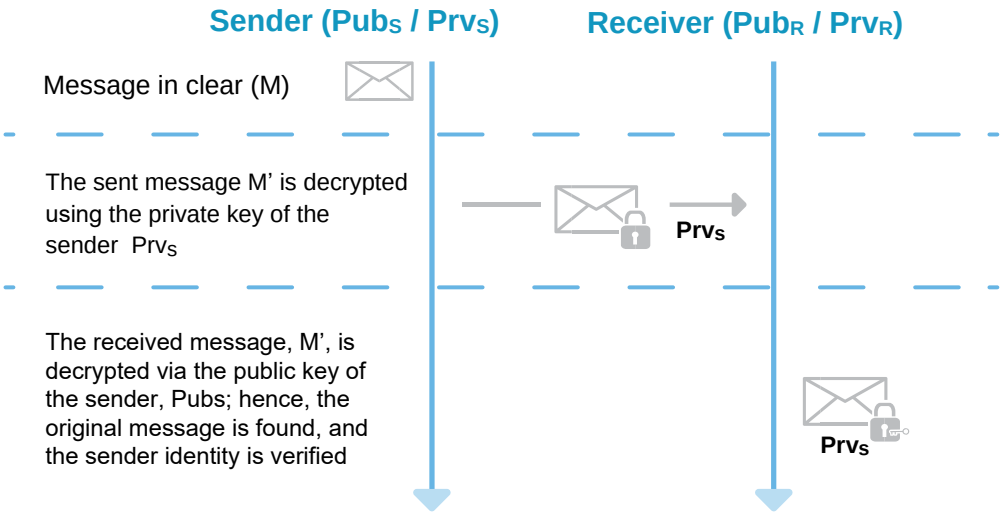
Figure 2: Generic Chain of Blocks

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

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2022.3149958, IEEE Access



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.

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 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:

$$h = H(M), M : message \quad (3)$$

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]:

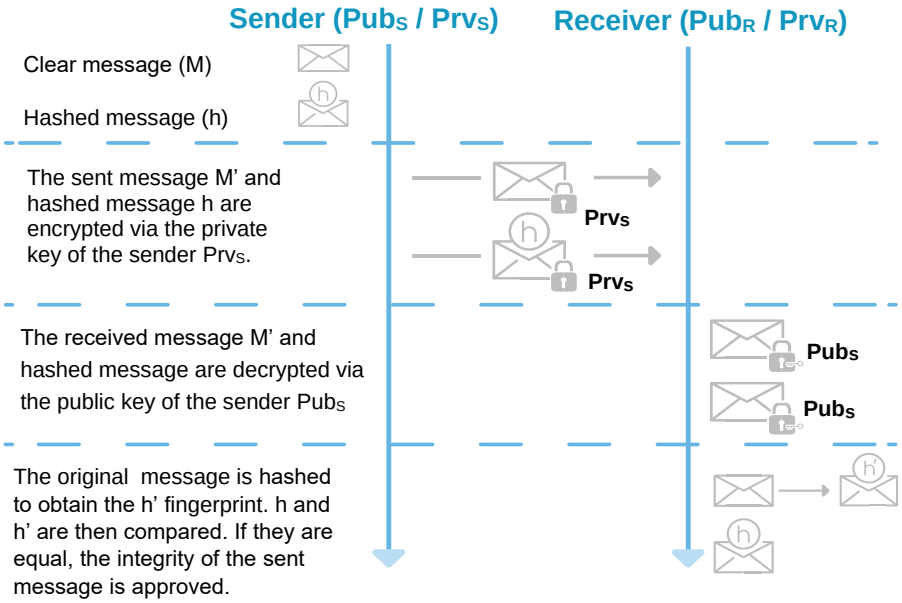
$$H(M) \neq H(N), if M \neq N, M, N : messages \quad (4)$$

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.

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.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2022.3149958, IEEE Access



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.

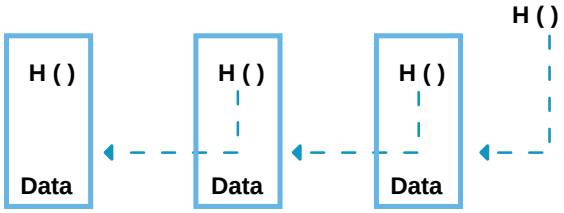


Figure 6: Hash Chain

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 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,

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2022.3149958, IEEE Access

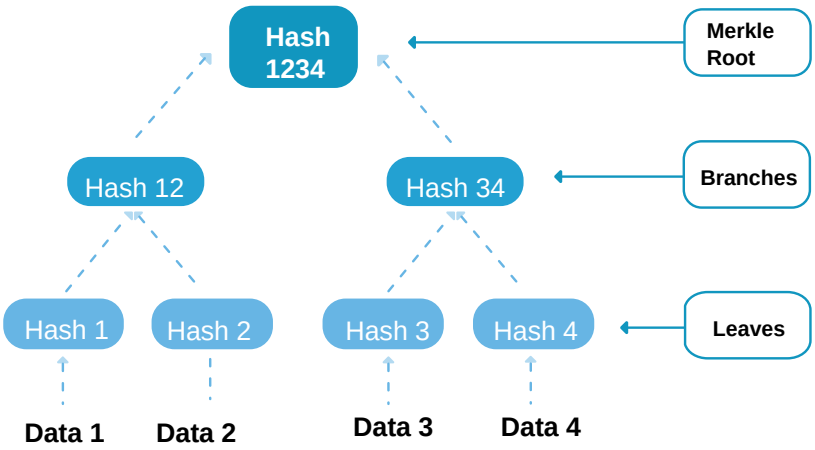


Figure 7: Hash Merkle Tree

"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.

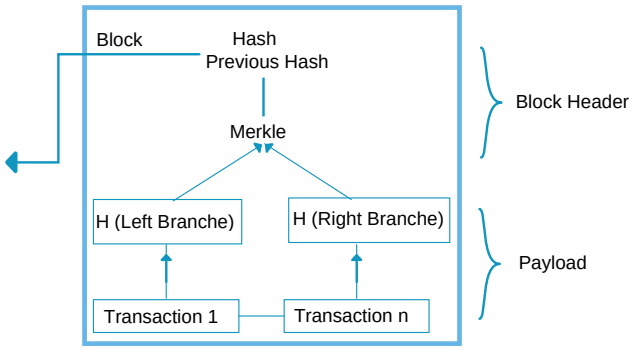


Figure 8: Block

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].

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2022.3149958, IEEE Access

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 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

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2022.3149958, IEEE Access

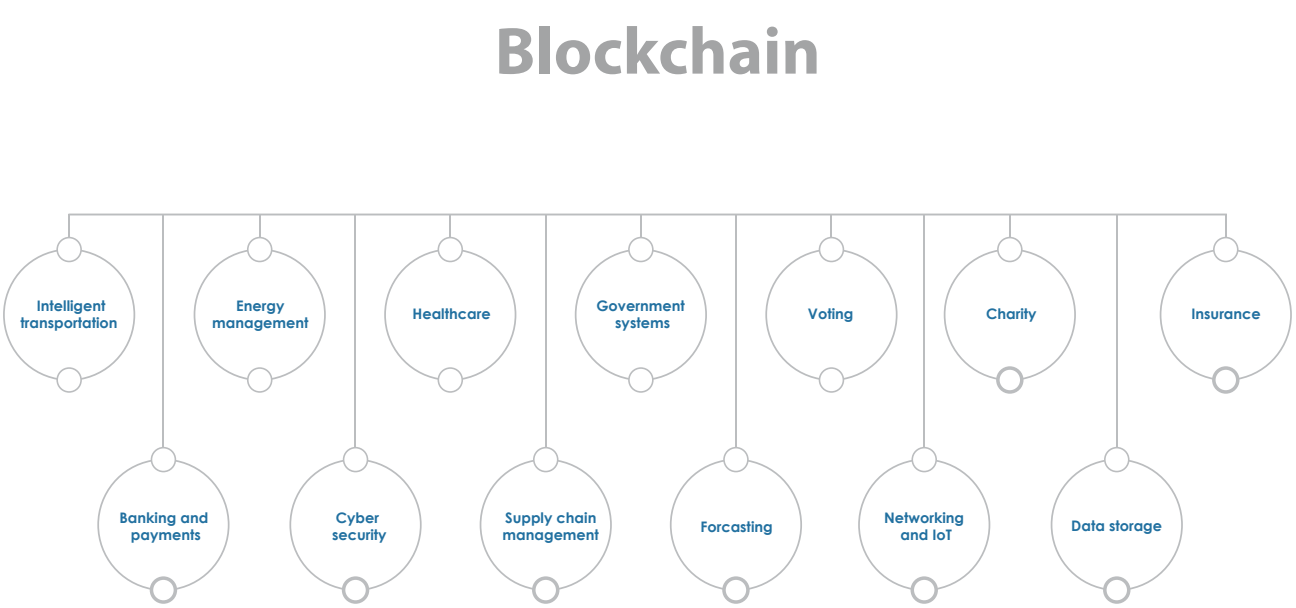


Figure 9: Blockchain Applications in Different Domains.

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 of 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. In the following, most of the known studied consensus protocols published in the literature are presented.

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

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2022.3149958, IEEE Access

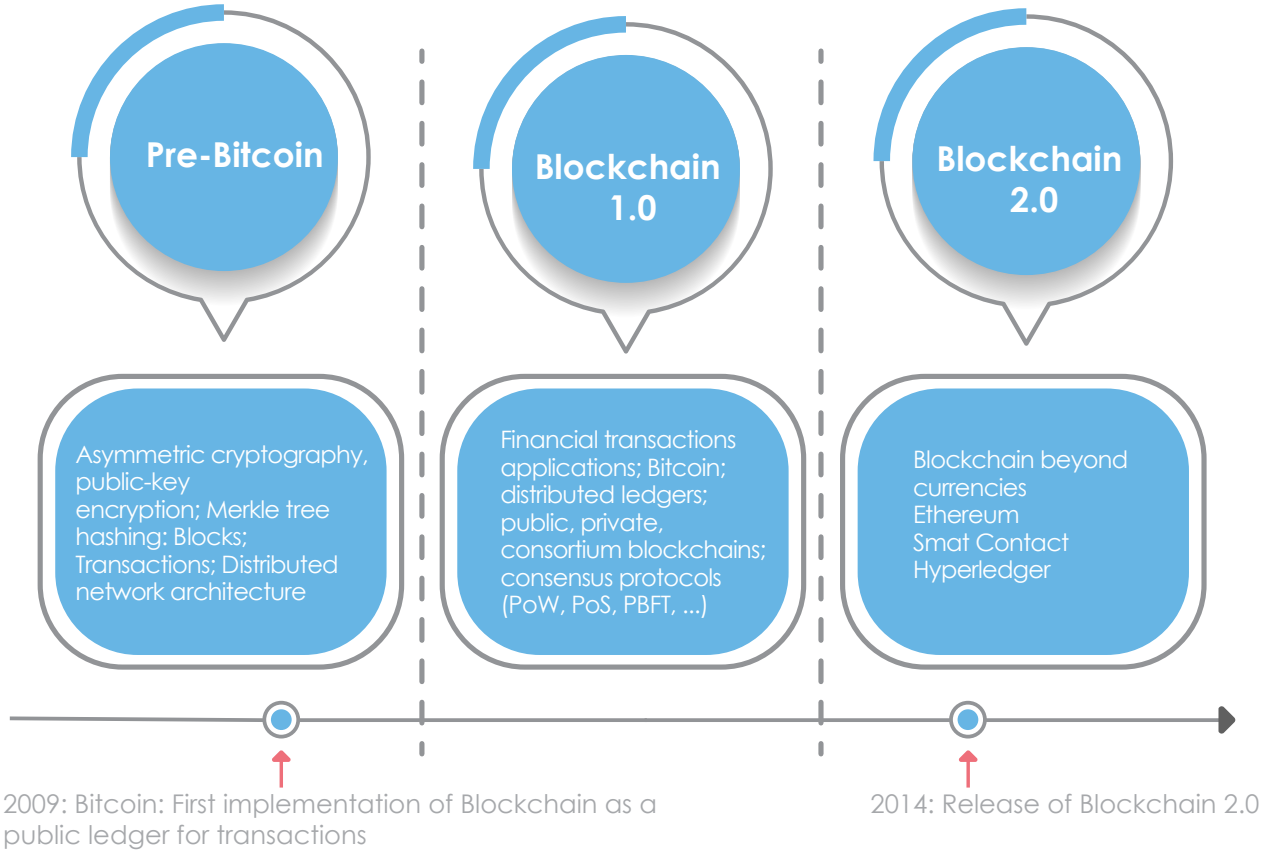


Figure 10: History of Blockchain technology.

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) represents a consensus mechanism based on a proof of ownership (i.e., the stake) [103], [104]; 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 saves more energy and accelerates transactions rates [54].

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

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2022.3149958, IEEE Access

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 is an autonomous actor that behaves transparently and predictably [93], [116].

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,

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2022.3149958, IEEE Access

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.

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

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. 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,

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2022.3149958, IEEE Access

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 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 analyzed the most distinct contributions of Blockchain to IoV based on an IoT–IoV 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.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2022.3149958, IEEE Access

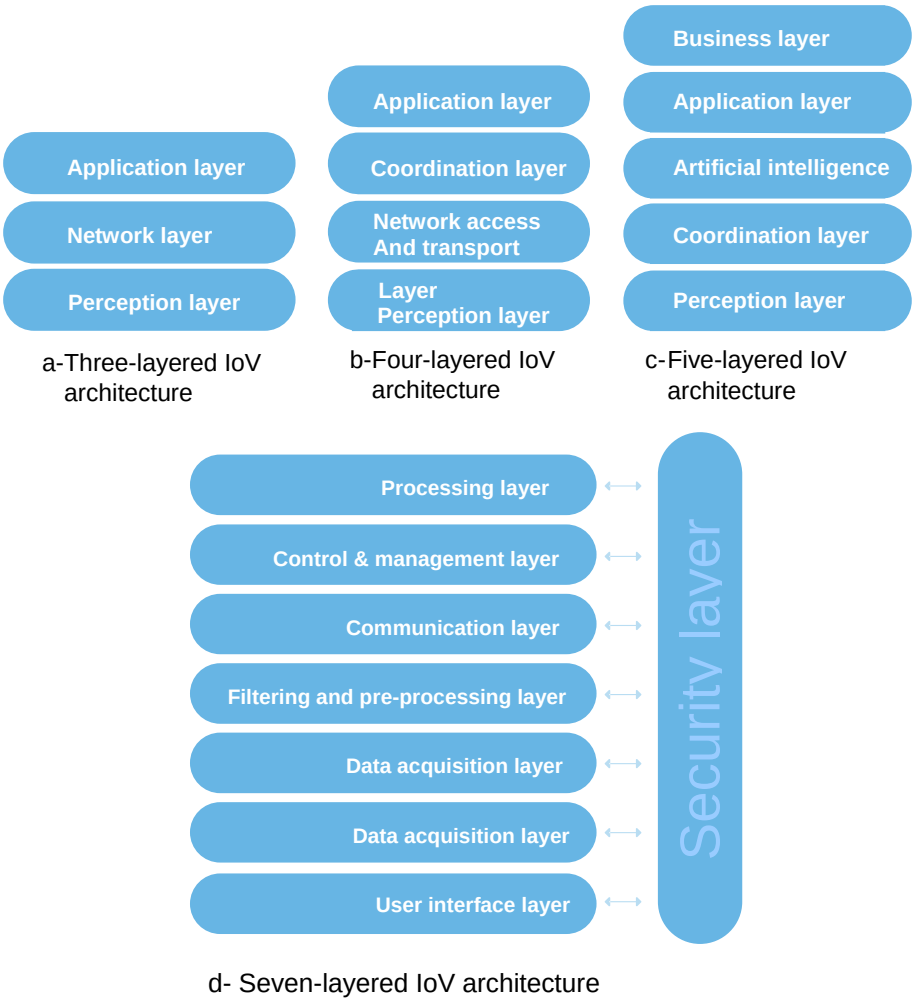


Figure 11: Existed IoV layered architecture models.

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.

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

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2022.3149958, IEEE Access

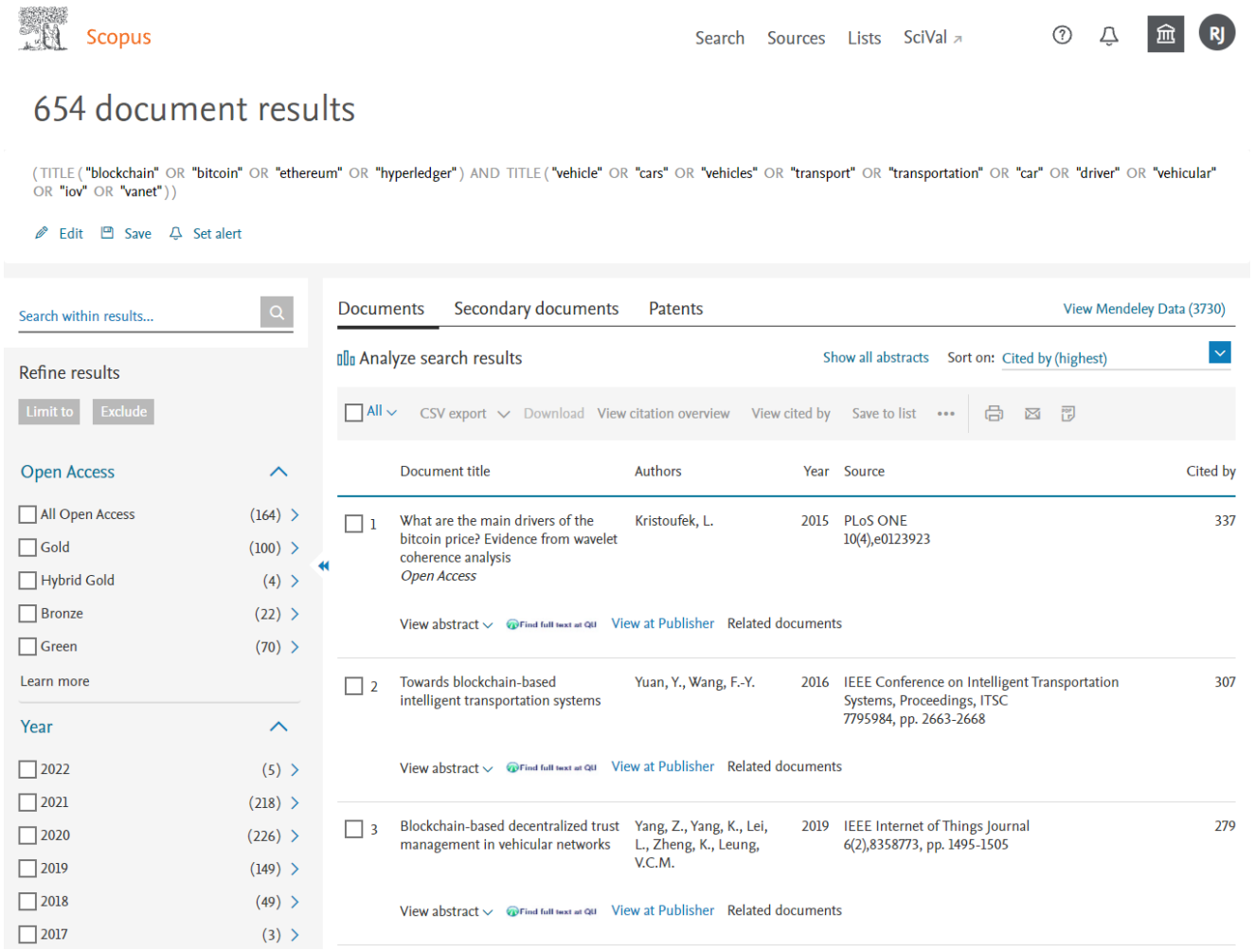


Figure 12: Scopus - Document search results.

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 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.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2022.3149958, IEEE Access

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 Blockchain technology is an attractive research focus in scientific communities.

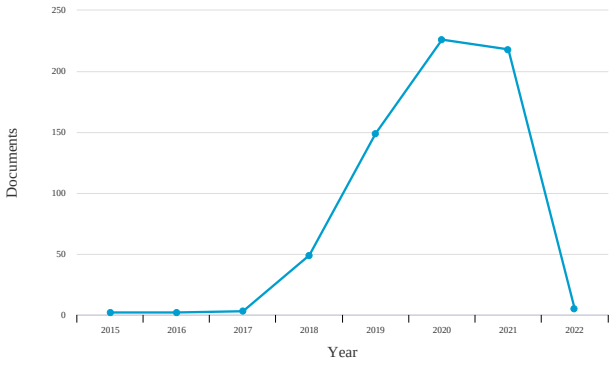


Figure 13: Documents per Year.

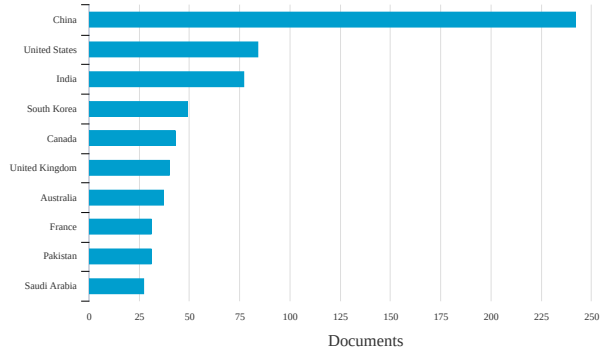


Figure 14: Documents by country.

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,

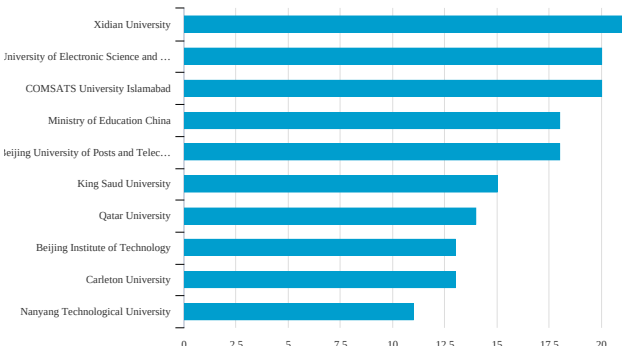


Figure 15: Documents by affiliation.

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.

The first paper (Yong Yuan and Fei-Yue Wang) [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. The second paper (Yang et al.) [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. The third paper (Lei et al.) [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. The fourth paper (Sharma et al.) [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. The last paper (Li et al.) [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,

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2022.3149958, IEEE Access

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.

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

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 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 authen-

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2022.3149958, IEEE Access

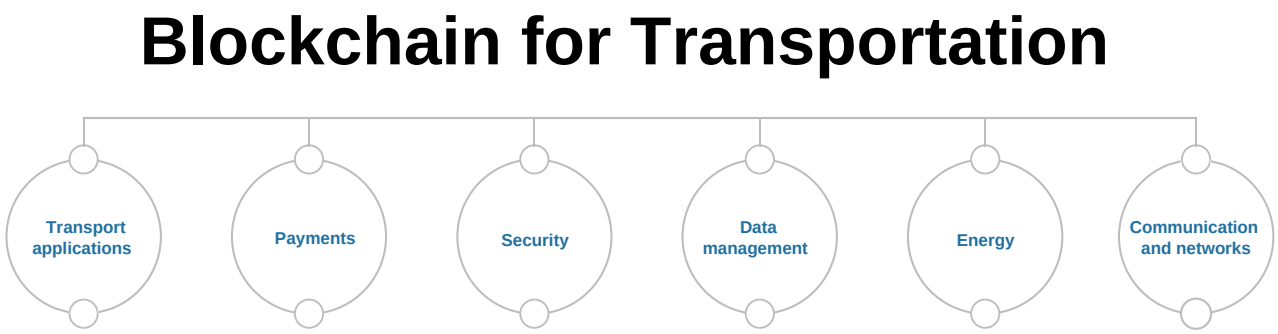


Figure 16: Blockchain for transportation.

tication, 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. TRANSPORTS 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 [243], [464], [465], car leasing [225], training and learning autonomous cars [226], and establishing trusted multiparty insurance [39]. They are also employed for the secure selling and buying of used cars [259] and the transparent dissemination of the usage history of motors for trading [227]. A smart contract-based platform for emerging transport services was proposed in [244]. 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 [271]. 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 [262]. 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 [265]. 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 are for smart charging or fueling services in vehicular networks using decentralized, private, or consortium Blockchain [285], [286], [289], [291], [293], [296], [297], [416], [466], [467]. As an application example, a simple selection mechanism of the charging unit for EV drivers is developed based on smart contracts [284]. In [295], 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

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2022.3149958, IEEE Access

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]–[223]
Transport applications	[39], [224]–[258]	-	[259]–[280]
Energy	[115], [281]–[301], [301]–[312]	[299]–[302], [313]–[315]	[115], [316]–[322]
Data management	[105], [159], [323]–[357]	[358], [359]	[105], [159], [323]–[348], [360]–[373]
Communication and network	[374]–[382]	[135], [157], [158], [378], [383]–[414]	[135], [157], [158], [383]–[406], [415]–[452]
Payments	[102], [107], [108], [453]–[455], [455]–[461]	[104], [106]	[102], [104], [106]–[108], [114], [453], [462], [463]

other selection criteria, such as actual battery status, traffic congestion, and service delay. Other research works focused on designing efficient energy trading frameworks for EVs [115], [281]–[283], [288], [290], [292], [294], [299]–[302], [321], [322]. In [283], 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 [313]. In the proposed architecture, 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 [115], [316]–[320]. For example, In [316], 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 [319], 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 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], [323]–[354], [360], 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 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 [324], [328], [334], [340], [341], [344], [345], [358], [359]. 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 [324]. A privacy scheme was then implemented to prove the correctness of collected and stored events as well as the registry of driver information. In [334], 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 [344], 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], [376]–[378], [383]–[411], [453], [468]–[471] was to enhance existing or suggest new communication protocols in vehicular networks, such as VANETs [374], [375], [390], [394], IoT based networks [385], IoV [157], [387], [389], [391], [472], [473], UAVs [388], SDN [157], [158], [412], 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 [383], a smart and trustworthy communication protocol using Blockchain technology for a cloud vehicular system was proposed. Successful exchanges were achieved as a

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2022.3149958, IEEE Access

result of applying an incentive mechanism that improves trust on the implied nodes. Jabbar et al. [474] developed a decentralized framework based on Blockchain technology (DISV); the DISV ([475], [476], [477]) 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 is a sub-system for obtaining information regarding the journey and vehicle ([478], [479]). The second sub-system, called driver drowsiness detection, aims to sense driver drowsiness by acquiring driver behavior information ([480], [481]). In [401], 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 [404], a hybrid architecture was developed to secure vehicle-to-vehicle and vehicle-to-infrastructure communications. In [405], 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 [453]. 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], [453] 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 [482]. 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 [483], 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 [484] is a multi-chain parallel computing Blockchain framework based on the concept of

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2022.3149958, IEEE Access

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. [485] proposed the introduction of parallel mining and changing the chain data structure to graph chain [486]. Toan et al. [487] proposed the use of a consensus mechanism of authorized PoSs to improve the efficiency of the Blockchain network. Fitz et al. [488] 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) [489] 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 [490], Proof of Search [491], Proof of Accuracy [492], Proof of Sincerity [493], Proof of Learning [494], Proof of Benefit [495], Proof of Experience [496], Proof of Evaluation [497], and Proof of Adjourn [498], 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 has been used in numerous areas, such as speech recognition, medical diagnosis, and computer vision [499]–[503]. 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 [504]. 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 impor-

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2022.3149958, IEEE Access

tantly, 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 [505] 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 [506]. 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. [349] 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. [254] 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 [507] 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 [508]. 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 includes data analysis, processing methodologies, and models (e.g., MapReduce processing and data clustering techniques) [509]. 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 is an excellent solution for big data problems [510]. 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 [511] and data sharing via smart contracts [512]. According to preliminary findings, Blockchain technology has the potential for significantly improving the performance and security of big data applications in the IoV era [407] [513] [514].

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,

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2022.3149958, IEEE Access

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 [515]. 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 [516]. 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 [517]. 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 [518]. 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 [519]. 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 [520]. 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 [521]. In this case, Blockchain technology can be utilized to construct trustworthy end-to-end network slices and facilitate resource management by network slice providers [522]. 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 [523]. 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 [524]. 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 [525]. 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 [526]. 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 [527], 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 [528] 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 publication was made possible by an NPRP award [NPRP11S-1228-170142] from the Qatar National Research Fund (a member of Qatar Foundation). The statements made herein are solely the responsibility of the authors.

References

[1] Sudeep Tanwar, Sudhanshu Tyagi, Ishan Budhiraja, and Neeraj Kumar. Tactile internet for autonomous vehicles: Latency and reliability analysis. IEEE Wireless Communications, 26(4):66–72, 2019.

[2] Surbhi Sharma and Baijnath Kaushik. A survey on internet of vehicles: Applications, security issues & solutions. Vehicular Communications, 20:100182, 2019.

[3] Yueyue Dai, Du Xu, Sabita Maharjan, Guanhua Qiao, and Yan Zhang. Artificial intelligence empowered edge computing and caching for internet of vehicles. IEEE Wireless Communications, 26(3):12–18, 2019.

[4] Ayyoub Lamssaggad, Nabil Benamar, Abdelhakim Senhaji Hafid, and Mounira Msahli. A survey on the current security landscape of intelligent transportation systems. IEEE Access, 9:9180–9208, 2021.

[5] Kan Zheng, Qiang Zheng, Periklis Chatzimisios, Wei Xiang, and Yiqing Zhou. Heterogeneous vehicular networking: A survey on architecture, challenges, and solutions. IEEE communications surveys & tutorials, 17(4):2377–2396, 2015.

[6] Georgios Karagiannis, Onur Altintas, Eylem Ekici, Geert Heijenk, Boangoat Jarupan, Kenneth Lin, and Timothy Weil. Vehicular networking: A survey and tutorial on requirements, architectures, challenges, standards and solutions. IEEE communications surveys & tutorials, 13(4):584–616, 2011.

[7] ERTICO – ITS Europe. https://ertico.com/, 2021. [Online; Available].

[8] cityverve. https://www.smartsustainablecities.uk/cityverve, 2021. [Online; Available].

[9] Michael Nofer, Peter Gomber, Oliver Hinz, and Dirk Schiereck. Blockchain. Business & Information Systems Engineering, 59(3):183–187, 2017.

[10] bitcoin.org. https://https://www.bitcoin.org/, 2021. [Online; Available].

[11] Ana Reyna, Cristian Martín, Jaime Chen, Enrique Soler, and Manuel Díaz. On blockchain and its integration with iot. challenges and opportunities. Future generation computer systems, 88:173–190, 2018.

[12] Sergey Smetanin, Aleksandr Ometov, Mikhail Komarov, Pavel Masek, and Yevgeni Koucheryavy. Blockchain evaluation approaches: State-of-the-art and future perspective. Sensors, 20(12):3358, 2020.

[13] Talal Ashraf Butt, Razi Iqbal, Khaled Salah, Moayad Aloqaily, and Yaser Jararweh. Privacy management in social internet of vehicles: review, challenges and blockchain based solutions. IEEE Access, 7:79694–79713, 2019.

[14] Vittorio Astarita, Vincenzo Pasquale Giofrè, Giovanni Mirabelli, and Vittorio Solina. A review of blockchain-based systems in transportation. Information, 11(1):21, 2020.

[15] Rajesh Gupta, Sudeep Tanwar, Neeraj Kumar, and Sudhanshu Tyagi. Blockchain-based security attack resilience schemes for autonomous vehicles in industry 4.0: A systematic review. Computers & Electrical Engineering, 86:106717, 2020.

[16] Sara El-Switi and Mohammad Qatawneh. Application of blockchain technology in used vehicle market: A review. In 2021 International Conference on Information Technology (ICIT), pages 49–54. IEEE, 2021.

[17] Sarah Iqbal, Rafidah Md Noor, and Asad Waqar Malik. A review of blockchain empowered vehicular network: Performance evaluation of trusted task offloading scheme. In 2021 IEEE 11th IEEE Symposium on Computer Applications & Industrial Electronics (ISCAIE), pages 367–371. IEEE, 2021.

[18] Leo Mendiboure, Mohamed Aymen Chalouf, and Francine Krief. Survey on blockchain-based applications in internet of vehicles. Computers & Electrical Engineering, 84:106646, 2020.

[19] Muhammad Baqer Mollah, Jun Zhao, Dusit Niyato, Yong Liang Guan, Chau Yuen, Sumei Sun, Kwok-Yan Lam, and Leong Hai Koh. Blockchain for the internet of vehicles towards intelligent transportation systems: A survey. IEEE Internet of Things Journal, 8(6):4157–4185, 2020.

[20] Xifeng Wang, Changqiao Xu, Zan Zhou, Shujie Yang, and Limin Sun. A survey of blockchain-based cybersecurity for vehicular networks. In 2020 International Wireless Communications and Mobile Computing (IWCMC), pages 740–745. IEEE, 2020.

[21] Mahdi Dibaei, Xi Zheng, Youhua Xia, Xiwei Xu, Alireza Jolfaei, Ali Kashif Bashir, Usman Tariq, Dongjin Yu, and Athanasios V Vasilakos. Investigating the prospect of leveraging blockchain and machine learning to secure vehicular networks: a survey. IEEE Transactions on Intelligent Transportation Systems, 2021.

[22] Branka Mikavica and Aleksandra Kostić-Ljubisavljević. Blockchain-based solutions for security, privacy, and trust management in vehicular networks: a survey. The Journal of Supercomputing, pages 1–56, 2021.

[23] Swati Megha, Hamza Salem, Enes Ayan, and Manuel Mazzara. A survey of blockchain solutions for autonomous vehicles ecosystems. In Journal of Physics: Conference Series, volume 1694, page 012024. IOP Publishing, 2020.

[24] Navid Khoshavi, Gabrielle Tristani, and Arman Sargolzaei. Blockchain applications to improve operation and security of transportation systems: A survey. Electronics, 10(5):629, 2021.

[25] Sathish Kumar, Sarveshwaran Velliangiri, Periyasami Karthikeyan, Saru Kumari, Sachin Kumar, and Muhammad Khurram Khan. A survey on the blockchain techniques for the internet of vehicles security. Transactions on Emerging Telecommunications Technologies, page e4317.

[26] Anderson Queiroz, Eduardo Oliveira, Maria Barbosa, and Kelvin Dias. A survey on blockchain and edge computing applied to the internet of vehicles. In 2020 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS), pages 1–6. IEEE, 2020.

[27] Chao Wang, Xiaoman Cheng, Jitong Li, Yunhua He, and Ke Xiao. A survey: applications of blockchain in the internet of vehicles. EURASIP Journal on Wireless Communications and Networking, 2021(1):1–16, 2021.

[28] Satoshi Nakamoto and A Bitcoin. A peer-to-peer electronic cash system. Bitcoin.–URL: https://bitcoin. org/bitcoin. pdf, 4, 2008.

[29] Arshdeep Bahga and Vijay K Madisetti. Blockchain platform for industrial internet of things. Journal of Software Engineering and Applications, 9(10):533–546, 2016.

[30] Junfeng Xie, Helen Tang, Tao Huang, F Richard Yu, Renchao Xie, Jiang Liu, and Yunjie Liu. A survey of blockchain technology applied to smart cities: Research issues and challenges. IEEE Communications Surveys & Tutorials, 21(3):2794–2830, 2019.

[31] Hong-Ning Dai, Zibin Zheng, and Yan Zhang. Blockchain for internet of things: A survey. IEEE Internet of Things Journal, 6(5):8076–8094, 2019.

[32] Hyperledger Iroha . https://www.hyperledger.org/projects/iroha, 2021. [Online; Available].

[33] Mehrdokht Pournader, Yangyan Shi, Stefan Seuring, and SC Lenny Koh. Blockchain applications in supply chains, transport and logistics: a systematic review of the literature. International Journal of Production Research, 58(7):2063–2081, 2020.

[34] S. A. Abeyratne and R. Monfared. Blockchain ready manufacturing supply chain using distributed ledger. International Journal of Research in Engineering and Technology, 05:1–10, 2016.

[35] Junghun Yoo, Youlim Jung, Donghwan Shin, Minhyo Bae, and Eunkyoung Jee. Formal modeling and verification of a federated byzantine agreement algorithm for blockchain platforms. In 2019 IEEE International Workshop on Blockchain Oriented Software Engineering (IWBOSE), pages 11–21. IEEE, 2019.

[36] Yong Yuan and Fei-Yue Wang. Towards blockchain-based intelligent transportation systems. In 2016 IEEE 19th International Conference on Intelligent Transportation Systems (ITSC), pages 2663–2668. IEEE, 2016.

[37] Blockchain: This is how bitcoin and ethereum are different - lupus consulting. https://lupusconsulting.com/2019/01/14/blockchain-this-is-how-bitcoin-and-ethereum-are-different/, 2021. [Online; Available].

[38] Bitcoin blockchain size 2009-2021 | statista. https://www.statista.com/statistics/647523/worldwide-bitcoin-blockchain-size/, 2021. [Online; Available].

[39] Zengxiang Li, Zhe Xiao, Quanqing Xu, Ekanut Sotthiwat, Rick Siow Mong Goh, and Xueping Liang. Blockchain and iot data analytics for fine-grained transportation insurance. In 2018 IEEE 24th International Conference on Parallel and Distributed Systems (ICPADS), pages 1022–1027. IEEE, 2018.

[40] Aiqing Zhang and Xiaodong Lin. Towards secure and privacy-preserving data sharing in e-health systems via consortium blockchain. Journal of medical systems, 42(8):140, 2018.

[41] Wenbo Wang, Dinh Thai Hoang, Zehui Xiong, Dusit Niyato, Ping Wang, Peizhao Hu, and Yonggang Wen. A survey on consensus mechanisms and mining management in blockchain networks. arXiv preprint arXiv:1805.02707, pages 1–33, 2018.

[42] Zhetao Li, Jiawen Kang, Rong Yu, Dongdong Ye, Qingyong Deng, and Yan Zhang. Consortium blockchain for secure energy trading in industrial internet of things. IEEE transactions on industrial informatics, 14(8):3690–3700, 2017.

[43] Jiawen Kang, Zehui Xiong, Dusit Niyato, Ping Wang, Dongdong Ye, and Dong In Kim. Incentivizing consensus propagation in proof-of-stake based consortium blockchain networks. IEEE Wireless Communications Letters, 8(1):157–160, 2018.

[44] Hyperledger Hyperledger-burrow . www.hyperledger.org/projects/hyperledger-burrow, 2021. [Online; Available].

[45] Hyperledger Fabric . https://www.hyperledger.org/projects/fabric, 2021. [Online; Available].

[46] Nitin Jirwan, Ajay Singh, and Dr Sandip Vijay. Review and analysis of cryptography techniques. International Journal of Scientific & Engineering Research, 4(3):1–6, 2013.

[47] Hyperledger Indy . https://www.hyperledger.org/projects/hyperledger-indy, 2021. [Online; Available].

[48] Hongwei Li, Rongxing Lu, Liang Zhou, Bo Yang, and Xuemin Shen. An efficient merkle-tree-based authentication scheme for smart grid. IEEE Systems Journal, 8(2):655–663, 2013.

[49] Merlinda Andoni, Valentin Robu, David Flynn, Simone Abram, Dale Geach, David Jenkins, Peter McCallum, and Andrew Peacock. Blockchain technology in the energy sector: A systematic review of challenges and opportunities. Renewable and Sustainable Energy Reviews, 100:143–174, 2019.

[50] Hyperledger Quilt. https://www.hyperledger.org/projects/quilt, 2021. [Online; Available].

[51] Hyperledger Sawtooth . https://www.hyperledger.org/projects/sawtooth, 2021. [Online; Available].

[52] Interledger Protocol (ILP). https://interledger.org/rfcs/0003-interledger-protocol, 2021. [Online; Available].

[53] Du Mingxiao, Ma Xiaofeng, Zhang Zhe, Wang Xiangwei, and Chen Qijun. A review on consensus algorithm of blockchain. In 2017 IEEE International Conference on Systems, Man, and Cybernetics (SMC), pages 2567–2572. IEEE, 2017.

[54] A (Short) Guide to Blockchain Consensus Protocols. https://www.coindesk.com/short-guide-blockchain-consensus-protocolsl, 2021. [Online; Available].

[55] Blockchain for financial services | ibm. https://www.ibm.com/blockchain/industries/financial-services, 2021. [Online; Available].

[56] Home - abra. https://www.abra.com/, 2021. [Online; Available].

[57] How barclays is exploring blockchain | innovation | barclays. https://home.barclays/news/2019/7/less-hype-and-more-collaboration--how-barclays-is-exploring-bloc/, 2021. [Online; Available].

[58] Press release: Paypal launches new service enabling users to buy, hold and sell cryptocurrency - oct 21, 2020. https://newsroom.paypal-corp.com/2020-10-21-PayPal-Launches-New-Service-Enabling-Users-to-Buy-Hold-and-Sell-Cryptocurrency, 2021. [Online; Available].

[59] Why mastercard is bringing crypto onto its network. https://www.mastercard.com/news/perspectives/2021/why-mastercard-is-bringing-crypto-onto-our-network/, 2021. [Online; Available].

[60] Crypto | money is evolving | visa. https://usa.visa.com/solutions/crypto.html, 2021. [Online; Available].

[61] Penta security systems inc. https://www.pentasecurity.com/, 2021. [Online; Available].

[62] Solidus labs | digital asset compliance. https://www.soliduslabs.com/, 2021. [Online; Available].

[63] Casa | the most secure storage for your bitcoin. https://www.keys.casa/, 2021. [Online; Available].

[64] Blockchain for supply chain - ibm blockchain | ibm. https://www.ibm.com/blockchain/supply-chain, 2021. [Online; Available].

[65] Shipchain thinks public blockchain can transform logistics for small business. https://www.forbes.com/sites/robertanzalone/2020/04/20/shipchain-thinks-public-blockchain-can-transform-logistics-for-small-business/?sh=2416d1cd3c1f, 2021. [Online; Available].

[66] Chronicled | automating transactions between trading partners. https://www.chronicled.com/, 2021. [Online; Available].

[67] Augur is the world's most accessible, low-fee, no-limit betting platform. https://augur.net/, 2021. [Online; Available].

[68] æternity - a blockchain for scalable, secure and decentralized æpps. https://aeternity.com/, 2021. [Online; Available].

[69] Ibm reveals proof of concept for blockchain-powered internet of things. https://www.coindesk.com/markets/2015/01/17/ibm-reveals-proof-of-concept-for-blockchain-powered-internet-of-things/, 2021. [Online; Available].

[70] Blockchain in insurance market size, share and global market forecast to 2023 | marketsandmarkets. https://www.marketsandmarkets.com/Market-Reports/blockchain-in-insurance-market-9714723.html, 2021. [Online; Available].

[71] Blockchain, a catalyst for new approaches in insurance: Part 1: Publications: Financial services: Industries: Pwc. https://www.pwc.com/gx/en/industries/financial-services/publications/blockchain-a-catalyst.html, 2021. [Online; Available].

[72] Storj - decentralized cloud storage. https://storj.io/, 2021. [Online; Available].

[73] Ipfs powers the distributed web. https://ipfs.io/#why, 2021. [Online; Available].

[74] bitgive |1st bitcoin and blockchain non profit charity organization. https://www.bitgivefoundation.org/, 2021. [Online; Available].

[75] Secure decentralized application development - follow my vote. https://followmyvote.com/, 2021. [Online; Available].

[76] Democracy earth. https://democracy.earth/#/, year = 2021, note =.

[77] Blockchain for government - ibm blockchain | ibm. https://www.ibm.com/blockchain/industries/government, 2021. [Online; Available].

[78] Blockchain in government and the public sector | consensys. https://consensys.net/blockchain-use-cases/government-and-the-public-sector/, 2021. [Online; Available].

[79] Blockchain in healthcare: Top 12 companies - the medical futurist. https://medicalfuturist.com/top-12-companies-bringing-blockchain-to-healthcare/, 2021. [Online; Available].

[80] doc.ai - get the full picture of your health. https://doc.ai/, 2021. [Online; Available].

[81] Iryo.network. https://iryo.network/#network, 2021. [Online; Available].

[82] Whole genome sequencing dna test | nebula genomics. https://nebula.org/whole-genome-sequencing-dna-test/, 2021. [Online; Available].

[83] Patientory inc | home. https://patientory.com/, 2021. [Online; Available].

[84] Blockchain in the energy sector | 2020 | siemens energy global. https://www.siemens-energy.com/global/en/news/magazine/2020/blockchain-opportunities-energy-sector.html, 2021. [Online; Available].

[85] Acciona uses blockchain to secure its energy management software. https://www.acciona.com/updates/news/acciona-uses-blockchain-to-secure-its-energy-management-software/?_adin=02021864894, 2021. [Online; Available].

[86] Jayesh Ahire. Blockchain: the future? Lulu. com, 2018.

[87] Ali Ghofrani, Esmat Zaidan, and Ammar Abulibdeh. Simulation and impact analysis of behavioral and socioeconomic dimensions of energy consumption. Energy, page 122502, 2021.

[88] Ali Ghofrani, Esmat Zaidan, and Mohsen Jafari. Reshaping energy policy based on social and human dimensions: an analysis of human-building interactions among societies in transition in gcc countries. Humanities and Social Sciences Communications, 8(1):1–26, 2021.

[89] Ubs bank, innogy and zf partner to provide blockchain-backed wallets for cars - econotimes. http://www.econotimes.com/UBS-bank-innogy-and-ZF-partner-to-provide-blockchain-backed-wallets-for-cars-471860, 2021. [Online; Available].

[90] Arcade city. https://arcade.city/, 2021. [Online; Available].

[91] Pierluigi Paganini. Hackers can remotely disable car alarm on Mitsubishi Outlander PHEV SUVs. https://securityaffairs.co/wordpress/48114/hacking/mitsubishi-outlander-phev-hacking.html/, 2016. [Online; Available: 07-Mai-2020].

[92] Yang Lu. Blockchain: A survey on functions, applications and open issues. Journal of Industrial Integration and Management, 3(04):1850015, 2018.

[93] Matthias Mettler. Blockchain technology in healthcare: The revolution starts here. In 2016 IEEE 18th international conference on e-health networking, applications and services (Healthcom), pages 1–3. IEEE, 2016.

[94] Suyash Gupta and Mohammad Sadoghi. Blockchain transaction processing., 2019.

[95] Heng Hou. The application of blockchain technology in e-government in china. In 2017 26th International Conference on Computer Communication and Networks (ICCCN), pages 1–4. IEEE, 2017.

[96] Stuart Haber and W. Scott Stornetta. How to time-stamp a digital document. J. Cryptology, 3:99–111, 1991.

[97] Nick Szabo. Bit gold . https://unenumerated.blogspot.com/2005/12/bit-gold.html, 2008. [Online; Available].

[98] Andriy Luntovskyy and Dietbert Guetter. Cryptographic technology blockchain and its applications. In The International Conference on Information and Telecommunication Technologies and Radio Electronics, pages 14–33. Springer, 2018.

[99] Usman W Chohan. The double spending problem and cryptocurrencies. Available at SSRN 3090174, 2017.

[100] Arthur Gervais, Ghassan O Karame, Karl Wüst, Vasileios Glykantzis, Hubert Ritzdorf, and Srdjan Capkun. On the security and performance

of proof of work blockchains. In Proceedings of the 2016 ACM SIGSAC conference on computer and communications security, pages 3–16, 2016.

[101] Lun Li, Jiqiang Liu, Lichen Cheng, Shuo Qiu, Wei Wang, Xiangliang Zhang, and Zonghua Zhang. Creditcoin: A privacy-preserving blockchain-based incentive announcement network for communications of smart vehicles. IEEE Transactions on Intelligent Transportation Systems, 19(7):2204–2220, 2018.

[102] Feng Gao, Liehuang Zhu, Meng Shen, Kashif Sharif, Zhiguo Wan, and Kui Ren. A blockchain-based privacy-preserving payment mechanism for vehicle-to-grid networks. IEEE network, 32(6):184–192, 2018.

[103] Hong Liu, Yan Zhang, and Tao Yang. Blockchain-enabled security in electric vehicles cloud and edge computing. IEEE Network, 32(3):78–83, 2018.

[104] Enes Erdin, Mumin Cebe, Kemal Akkaya, Senay Solak, Eyuphan Bulut, and Selcuk Uluagac. Building a private bitcoin-based payment network among electric vehicles and charging stations. In 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), pages 1609–1615. IEEE, 2018.

[105] Ao Lei, Haitham Cruickshank, Yue Cao, Philip Asuquo, Chibueze P Anyigor Ogah, and Zhili Sun. Blockchain-based dynamic key management for heterogeneous intelligent transportation systems. IEEE Internet of Things Journal, 4(6):1832–1843, 2017.

[106] Mengting Liu, Yinglei Teng, F Richard Yu, Victor CM Leung, and Mei Song. Deep reinforcement learning based performance optimization in blockchain-enabled internet of vehicle. In ICC 2019-2019 IEEE International Conference on Communications (ICC), pages 1–6. IEEE, 2019.

[107] Seohyeon Jeong, Nhu-Ngoc Dao, Yunseong Lee, Cheol Lee, and Sungrae Cho. Blockchain based billing system for electric vehicle and charging station. In 2018 Tenth International Conference on Ubiquitous and Future Networks (ICUFN), pages 308–310. IEEE, 2018.

[108] Wei Hu, Wenhui Yao, Yawei Hu, and Huanhao Li. Collaborative optimization of distributed scheduling based on blockchain consensus mechanism considering battery-swap stations of electric vehicles. IEEE Access, 7:137959–137967, 2019.

[109] Miguel Castro, Barbara Liskov, et al. Practical byzantine fault tolerance. In OSDI, volume 99, pages 173–186, 1999.

[110] Leslie Lamport, Robert Shostak, and Marshall Pease. The byzantine generals problem. In Concurrency: the Works of Leslie Lamport, pages 203–226. 2019.

[111] Li Zhang and Qinwei Li. Research on consensus efficiency based on practical byzantine fault tolerance. In 2018 10th International Conference on Modelling, Identification and Control (ICMIC), pages 1–6. IEEE, 2018.

[112] Intel is winning over blockchain critics by reimagining Bitcoin's DNA. www.coindesk.com/intel-winning-blockchain-critics-reimagining-bitcoins-dnal, 2016. [Online; Available].

[113] The five most popular asic miners for cryptocurrency. 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, year = 2021, note =.

[114] D Dayana Baby, Krishnan C Sivarama, Sarah Patrick Cimryn, and Venkateswaran N. Tracking and monitoring of vehicles and a stable and secure tolltax payment methodology based on blockchain enabled cryptocurrency e-wallets. International Journal of Engineering and Advanced Technology (IJEAT), 8:685–690, 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 Transactions on Systems, Man, and Cybernetics: Systems, 50(1):43–57, 2020.

[116] Y. Wang, Z. Su, Q. Xu, and N. Zhang. Contract based energy blockchain for secure electric vehicles charging in smart community. In 2018 IEEE 16th Intl Conf on Dependable, Autonomic and Secure Computing, 16th Intl Conf on Pervasive Intelligence and Computing, 4th Intl Conf on Big Data Intelligence and Computing and Cyber Science and Technology Congress(DASC/PiCom/DataCom/CyberSciTech), pages 323–327, 2018.

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

[118] Ethereum blockchain as a service now on azure | microsoft, 2021. [Online; Available].

[119] Hyperledger. https://www.ibm.com/blockchain/hyperledge, 2021. [Online; Available].

[120] monax.io. https://monax.io/, 2021. [Online; Available].

[121] Hyperledger Caliper. https://www.hyperledger.org/projects/caliper, 2021. [Online; Available].

[122] Hyperledger Cello. https://www.hyperledger.org/projects/cello, 2021. [Online; Available].

[123] Hyperledger Explore. https://www.hyperledger.org/projects/explorer, 2021. [Online; Available].

[124] Dalila Boughaci and Omar Boughaci. A comparative study of three blockchain emerging technologies: Bitcoin, ethereum and hyperledger. In International Conference on Computing, pages 3–7. Springer, 2019.

[125] Leo Mendiboure, Mohamed Aymen Chalouf, and Francine Krief. Survey on blockchain-based applications in internet of vehicles. Computers & Electrical Engineering, 84:106646, 2020.

[126] Ruhi Taş and Ömer Özgür Tanrıöver. Building a decentralized application on the ethereum blockchain. In 2019 3rd International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT), pages 1–4. IEEE, 2019.

[127] Miao Wu, Ting-Jie Lu, Fei-Yang Ling, Jing Sun, and Hui-Ying Du. Research on the architecture of internet of things. In 2010 3rd international conference on advanced computer theory and engineering (ICACTE), volume 5, pages V5–484. IEEE, 2010.

[128] Rafiullah Khan, Sarmad Ullah Khan, Rifaqat Zaheer, and Shahid Khan. Future internet: the internet of things architecture, possible applications and key challenges. In 2012 10th international conference on frontiers of information technology, pages 257–260. IEEE, 2012.

[129] Livinus Tuyisenge, Marwane Ayaida, Samir Tohme, and Lissan-Eddine Afilal. Network architectures in internet of vehicles (iov): Review, protocols analysis, challenges and issues. In International Conference on Internet of Vehicles, pages 3–13. Springer, 2018.

[130] Pallavi Sethi and Smruti R Sarangi. Internet of things: architectures, protocols, and applications. Journal of Electrical and Computer Engineering, 2017, 2017.

[131] Marcos A Pisching, Marcosiris AO Pessoa, Fabrício Junqueira, Diolino J dos Santos Filho, and Paulo E Miyagi. An architecture based on rami 4.0 to discover equipment to process operations required by products. Computers & Industrial Engineering, 125:574–591, 2018.

[132] Marcela G dos Santos, Darine Ameyed, Fabio Petrillo, Fehmi Jaafar, and Mohamed Cheriet. Internet of things architectures: A comparative study. arXiv preprint arXiv:2004.12936, 2020.

[133] Scopus - Document search results. http://bit.ly/BiovScopusresults, 2021. [Online; Available].

[134] Zhe Yang, Kan Yang, Lei Lei, Kan Zheng, and Victor CM Leung. Blockchain-based decentralized trust management in vehicular networks. IEEE Internet of Things Journal, 6(2):1495–1505, 2018.

[135] Pradip Kumar Sharma, Seo Yeon Moon, and Jong Hyuk Park. Block-vn: A distributed blockchain based vehicular network architecture in smart city. Journal of information processing systems, 13(1), 2017.

[136] Zhe Yang, Kan Zheng, Kan Yang, and Victor CM Leung. A blockchain-based reputation system for data credibility assessment in vehicular networks. In 2017 IEEE 28th annual international symposium on personal, indoor, and mobile radio communications (PIMRC), pages 1–5. IEEE, 2017.

[137] Nisha Malik, Priyadarsi Nanda, Arushi Arora, Xiangjian He, and Deepak Puthal. Blockchain based secured identity authentication and expeditious revocation framework for vehicular networks. In 2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE), pages 674–679. IEEE, 2018.

[138] Mirador Labrador and Weiyan Hou. Implementing blockchain technology in the internet of vehicle (iov). In 2019 International Conference on Intelligent Computing and its Emerging Applications (ICEA), pages 5–10. IEEE, 2019.

[139] Tim Reimers, Felix Leber, and Ulrike Lechner. Integration of blockchain and internet of things in a car supply chain. In 2019 IEEE International Conference on Decentralized Applications and Infrastructures (DAPPCON), pages 146–151. IEEE, 2019.

[140] Ahmad Mostafa. Vanet blockchain: A general framework for detecting malicious vehicles. J. Commun, 14(5):356–362, 2019.

[141] Kuan Zhang, Xiaohui Liang, Rongxing Lu, and Xuemin Shen. Sybil attacks and their defenses in the internet of things. IEEE Internet of Things Journal, 1(5):372–383, 2014.

[142] Geetanjali Rathee, Ashutosh Sharma, Razi Iqbal, Moayad Aloqaily, Naveen Jaglan, and Rajiv Kumar. A blockchain framework for securing connected and autonomous vehicles. Sensors, 19(14):3165, 2019.

[143] Jaewon Noh, Sangil Jeon, and Sunghyun Cho. Distributed blockchain-based message authentication scheme for connected vehicles. Electronics, 9(1):74, 2020.

[144] Sara Nadeem, Muhammad Rizwan, Fahad Ahmad, and Jaweria Manzoor. Securing cognitive radio vehicular ad hoc network with fog node based distributed blockchain cloud architecture. INTERNATIONAL JOURNAL OF ADVANCED COMPUTER SCIENCE AND APPLICATIONS, 10(1):288–295, 2019.

[145] Yuancheng Li and Baiji Hu. A consortium blockchain-enabled secure and privacy-preserving optimized charging and discharging trading scheme for electric vehicles. IEEE Transactions on Industrial Informatics, 17(3):1968–1977, 2020.

[146] Marcello Cinque, Christian Esposito, Stefano Russo, and Oscar Tamburis. Blockchain-empowered decentralised trust management for the internet of vehicles security. Computers & Electrical Engineering, 86:106722, 2020.

[147] Rakesh Shrestha, Rojeena Bajracharya, Anish P Shrestha, and Seung Yeob Nam. A new type of blockchain for secure message exchange in vanet. Digital communications and networks, 6(2):177–186, 2020.

[148] Biwen Chen, Libing Wu, Huaqun Wang, Lu Zhou, and Debiao He. A blockchain-based searchable public-key encryption with forward and backward privacy for cloud-assisted vehicular social networks. IEEE Transactions on Vehicular Technology, 69(6):5813–5825, 2019.

[149] Lewis Nkenyereye, Bayu Adhi Tama, Muhammad K Shahzad, and Yoon-Ho Choi. Secure and blockchain-based emergency driven message protocol for 5g enabled vehicular edge computing. Sensors, 20(1):154, 2020.

[150] AFM Akhter, Mohiuddin Ahmed, AFM Shah, Adnan Anwar, and Ahmet Zengin. A secured privacy-preserving multi-level blockchain framework for cluster based vanet. Sustainability, 13(1):400, 2021.

[151] Rajesh Gupta, Aparna Kumari, and Sudeep Tanwar. A taxonomy of blockchain envisioned edge-as-a-connected autonomous vehicles. Transactions on Emerging Telecommunications Technologies, page e4009, 2020.

[152] Zhuo Ma, Junwei Zhang, Yongzhen Guo, Yang Liu, Ximeng Liu, and Wei He. An efficient decentralized key management mechanism for vanet with blockchain. IEEE Transactions on Vehicular Technology, 69(6):5836–5849, 2020.

[153] Sanjeev Kumar Dwivedi, Ruhul Amin, Satyanarayana Vollala, and Rashmi Chaudhry. Blockchain-based secured event-information sharing protocol in internet of vehicles for smart cities. Computers & Electrical Engineering, 86:106719, 2020.

[154] Yuhong Li, Kun Ouyang, Nanxuan Li, Rahim Rahmani, Haojun Yang, and Yiwei Pei. A blockchain-assisted intelligent transportation system promoting data services with privacy protection. Sensors, 20(9):2483, 2020.

[155] Debashis Das, Sourav Banerjee, and Utpal Biswas. A secure vehicle theft detection framework using blockchain and smart contract. Peer-to-Peer Networking and Applications, 14(2):672–686, 2021.

[156] Merzougui Salah Eddine, Mohamed Amine Ferrag, Othmane Friha, and Leandros Maglaras. Easbf: An efficient authentication scheme over blockchain for fog computing-enabled internet of vehicles. Journal of Information Security and Applications, 59:102802, 2021.

[157] Jianbin Gao, Kwame Opuni-Boachie Obour Agyekum, Emmanuel Boateng Sifah, Kingsley Nketia Acheampong, Qi Xia, Xiaojiang Du, Mohsen Guizani, and Hu Xia. A blockchain-sdn-enabled internet of vehicles environment for fog computing and 5g networks. IEEE Internet of Things Journal, 7(5):4278–4291, 2019.

[158] Dajun Zhang, F Richard Yu, and Ruizhe Yang. Blockchain-based distributed software-defined vehicular networks: A dueling deep $\mathcal{Q}$-learning approach. IEEE Transactions on Cognitive Communications and Networking, 5(4):1086–1100, 2019.

[159] LEE Sang-Oun, JUNG Hyunseok, and Bosuk Han. Security assured vehicle data collection platform by blockchain: Service provider's perspective. In 2019 21st International Conference on Advanced Communication Technology (ICACT), pages 265–268. IEEE, 2019.

[160] Xiaohong Huang, Cheng Xu, Pengfei Wang, and Hongzhe Liu. Lnsc: A security model for electric vehicle and charging pile management based on blockchain ecosystem. IEEE Access, 6:13565–13574, 2018.

[161] Meng Li, Liehuang Zhu, and Xiaodong Lin. Efficient and privacy-preserving carpooling using blockchain-assisted vehicular fog computing. IEEE Internet of Things Journal, 6(3):4573–4584, 2018.

[162] Hakima Khelifi, Senlin Luo, Boubakr Nour, Hassine Moungla, and Syed Hassan Ahmed. Reputation-based blockchain for secure ndn caching in vehicular networks. In 2018 IEEE Conference on Standards for Communications and Networking (CSCN), pages 1–6. IEEE, 2018.

[163] Youcef Yahiatene and Abderrezak Rachedi. Towards a blockchain and software-defined vehicular networks approaches to secure vehicular social network. In 2018 IEEE Conference on Standards for Communications and Networking (CSCN), pages 1–7. IEEE, 2018.

[164] Liviu-Adrian Hîrtan and Ciprian Dobre. Blockchain privacy-preservation in intelligent transportation systems. In 2018 IEEE International Conference on Computational Science and Engineering (CSE), pages 177–184. IEEE, 2018.

[165] Jiawen Kang, Zehui Xiong, Dusit Niyato, Dongdong Ye, Dong In Kim, and Jun Zhao. Toward secure blockchain-enabled internet of vehicles: Optimizing consensus management using reputation and contract theory. IEEE Transactions on Vehicular Technology, 68(3):2906–2920, 2019.

[166] Gianmarco Baldini, José L Hernández-Ramos, Gary Steri, and Sara N Matheu. Zone keys trust management in vehicular networks based on blockchain. In 2019 Global IoT Summit (GIoTS), pages 1–6. IEEE, 2019.

[167] Isaac J Jensen, Daisy Flora Selvaraj, and Prakash Ranganathan. Blockchain technology for networked swarms of unmanned aerial vehicles (uavs). In 2019 IEEE 20th International Symposium on" A World of Wireless, Mobile and Multimedia Networks"(WoWMoM), pages 1–7. IEEE, 2019.

[168] Junfei Qiu, David Grace, Guoru Ding, Junnan Yao, and Qihui Wu. Blockchain-based secure spectrum trading for unmanned-aerial-vehicle-assisted cellular networks: An operator's perspective. IEEE Internet of Things Journal, 7(1):451–466, 2019.

[169] Yingying Yao, Xiaolin Chang, Jelena Mišić, Vojislav B Mišić, and Lin Li. Bla: Blockchain-assisted lightweight anonymous authentication for distributed vehicular fog services. IEEE Internet of Things Journal, 6(2):3775–3784, 2019.

[170] Haoye Chai, Supeng Leng, Ke Zhang, and Sun Mao. Proof-of-reputation based-consortium blockchain for trust resource sharing in internet of vehicles. IEEE Access, 7:175744–175757, 2019.

[171] Farah Kandah, Brennan Huber, Anthony Skjellum, and Amani Altarawneh. A blockchain-based trust management approach for connected autonomous vehicles in smart cities. In 2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC), pages 0544–0549. IEEE, 2019.

[172] Xiaoliang Wang, Pengjie Zeng, Nick Patterson, Frank Jiang, and Robin Doss. An improved authentication scheme for internet of vehicles based on blockchain technology. IEEE access, 7:45061–45072, 2019.

[173] Jiawen Kang, Zehui Xiong, Dusit Niyato, and Dong In Kim. Incentivizing secure block verification by contract theory in blockchain-enabled vehicular networks. In ICC 2019-2019 IEEE International Conference on Communications (ICC), pages 1–7. IEEE, 2019.

[174] Ming Li, Jian Weng, Anjia Yang, Jia-Nan Liu, and Xiaodong Lin. Toward blockchain-based fair and anonymous ad dissemination in vehicular networks. IEEE Transactions on Vehicular Technology, 68(11):11248–11259, 2019.

[175] Yi Mu, Fatemeh Rezaeibagha, and Ke Huang. Policy-driven blockchain and its applications for transport systems. IEEE Transactions on Services Computing, 13(2):230–240, 2019.

[176] Qi Feng, Debiao He, Sherali Zeadally, and Kaitai Liang. Bpas: Blockchain-assisted privacy-preserving authentication system for vehicular ad hoc networks. IEEE Transactions on Industrial Informatics, 16(6):4146–4155, 2019.

[177] Xinghua Li, Yunwei Wang, Pandi Vijayakumar, Debiao He, Neeraj Kumar, and Jianfeng Ma. Blockchain-based mutual-healing group key distribution scheme in unmanned aerial vehicles ad-hoc network. IEEE Transactions on Vehicular Technology, 68(11):11309–11322, 2019.

[178] Biwen Chen, Libing Wu, Huaqun Wang, Lu Zhou, and Debiao He. A blockchain-based searchable public-key encryption with forward and backward privacy for cloud-assisted vehicular social networks. IEEE Transactions on Vehicular Technology, 2019.

[179] Meng Shen, Jie Zhang, Liehuang Zhu, Ke Xu, and Xiangyun Tang. Secure svm training over vertically-partitioned datasets using consortium blockchain for vehicular social networks. IEEE Transactions on Vehicular Technology, 2019.

[180] Talal Ashraf Butt, Razi Iqbal, Khaled Salah, Moayad Aloqaily, and Yaser Jararweh. Privacy management in social internet of vehicles: review, challenges and blockchain based solutions. IEEE Access, 7:79694–79713, 2019.

[181] Shaoyong Guo, Xing Hu, Ziqiang Zhou, Xinyan Wang, Feng Qi, and Lifang Gao. Trust access authentication in vehicular network based on blockchain. China Communications, 16(6):18–30, 2019.

[182] Qianlong Wang, Tianxi Ji, Yifan Guo, Lixing Yu, Xuhui Chen, and Pan Li. Trafficchain: A blockchain-based secure and privacy-preserving traffic map. IEEE Access, 8:60598–60612, 2020.

[183] Christian Kaiser, Marco Steger, Ali Dorri, Andreas Festl, Alexander Stocker, Michael Fellmann, and Salil Kanhere. Towards a privacy-preserving way of vehicle data sharing–a case for blockchain technology? In International Forum on Advanced Microsystems for Automotive Applications, pages 111–122. Springer, 2018.

[184] Liudmila Zavolokina, Noah Zani, and Gerhard Schwabe. Why should i trust a blockchain platform? designing for trust in the digital car dossier. In International Conference on Design Science Research in Information Systems and Technology, pages 269–283. Springer, 2019.

[185] Iván García-Magariño, Raquel Lacuesta, Muttukrishnan Rajarajan, and Jaime Lloret. Security in networks of unmanned aerial vehicles for surveillance with an agent-based approach inspired by the principles of blockchain. Ad Hoc Networks, 86:72–82, 2019.

[186] Rajat Chaudhary, Anish Jindal, Gagangeet Singh Aujla, Shubhani Aggarwal, Neeraj Kumar, and Kim-Kwang Raymond Choo. Best: Blockchain-based secure energy trading in sdn-enabled intelligent transportation system. Computers & Security, 85:288–299, 2019.

[187] Ikram Ali, Mwitende Gervais, Emmanuel Ahene, and Fagen Li. A blockchain-based certificateless public key signature scheme for vehicle-to-infrastructure communication in vanets. Journal of Systems Architecture, 99:101636, 2019.

[188] Alexey Busygin, Artem Konoplev, Maxim Kalinin, and Dmitry Zegzhda. Floating genesis block enhancement for blockchain based routing between connected vehicles and software-defined vanet security services. In Proceedings of the 11th International Conference on Security of Information and Networks, pages 1–2, 2018.

[189] Adnan Imeri, Christophe Feltus, Djamel Khadraoui, Nazim Agoulmine, and Damien Nicolas. Solving the trust issues in the process of transportation of dangerous goods by using blockchain technology. In Proceedings of the 11th International Conference on Security of Information and Networks, pages 1–2, 2018.

[190] Miro Petković and Igor Vujović. Blockchain security of autonomous maritime transport. Journal of Applied Engineering Science, 17(3):333–337, 2019.

[191] Youcef Yahiatene, Abderrezak Rachedi, Mohamed Amine Riahla, Djamel Eddine Menacer, and Farid Nait-Abdesselam. A blockchain-based framework to secure vehicular social networks. Transactions on Emerging Telecommunications Technologies, 30(8):e3650, 2019.

[192] Ning Zhao, Hao Wu, and Xiaonan Zhao. Consortium blockchain-based secure software defined vehicular network. Mobile Networks and Applications, 25(1):314–327, 2020.

[193] Rakesh Shrestha and Seung Yeob Nam. Regional blockchain for vehicular networks to prevent 51% attacks. IEEE Access, 7:95021–95033, 2019.

[194] Yi Yang, Debiao He, Huaqun Wang, and Lu Zhou. An efficient blockchain-based batch verification scheme for vehicular ad hoc networks. Transactions on Emerging Telecommunications Technologies, 2019.

[195] Yuling Chen, Xiaohan Hao, Wei Ren, and Yi Ren. Traceable and authenticated key negotiations via blockchain for vehicular communications. Mobile Information Systems, 2019, 2019.

[196] Razi Iqbal, Talal Ashraf Butt, Muhammad Afzaal, and Khaled Salah. Trust management in social internet of vehicles: Factors, challenges, blockchain, and fog solutions. International Journal of Distributed Sensor Networks, 15(1):1550147719825820, 2019.

[197] Mirador Labrador and Weiyan Hou. Security mechanism for vehicle identification and transaction authentication in the internet of vehicle (iov) scenario: A blockchain based model. Journal of Computer Science, 15, 02 2019.

[198] Xinshu Ma, Chunpeng Ge, and Zhe Liu. Blockchain-enabled privacy-preserving internet of vehicles: Decentralized and reputation-based network architecture. In International Conference on Network and System Security, pages 336–351. Springer, 2019.

[199] Wei Ou, Mingwei Deng, and Entao Luo. A decentralized and anonymous data transaction scheme based on blockchain and zero-knowledge proof in vehicle networking (workshop paper). In International Conference on Collaborative Computing: Networking, Applications and Worksharing, pages 712–726. Springer, 2019.

[200] Lucas Davi, Denis Hatebur, Maritta Heisel, and Roman Wirtz. Combining safety and security in autonomous cars using blockchain technologies. In International Conference on Computer Safety, Reliability, and Security, pages 223–234. Springer, 2019.

[201] Serkan Ayvaz and Salih Cemil Cetin. Witness of things. International Journal of Intelligent Unmanned Systems, 2019.

[202] Kuljeet Kaur, Sahil Garg, Georges Kaddoum, François Gagnon, and Syed Hassan Ahmed. Blockchain-based lightweight authentication mechanism for vehicular fog infrastructure. In 2019 IEEE International Conference on Communications Workshops (ICC Workshops), pages 1–6. IEEE, 2019.

[203] Anil Saini, Shreyansh Sharma, Palash Jain, Vikash Sharma, and Arvind Kumar Khandelwal. A secure priority vehicle movement based on blockchain technology in connected vehicles. In Proceedings of the 12th International Conference on Security of Information and Networks, pages 1–8, 2019.

[204] Chi-Sheng Shih, Wei-Yu Hsieh, and Chia-Lung Kao. Traceability for vehicular network real-time messaging based on blockchain technology. J. Wirel. Mob. Networks Ubiquitous Comput. Dependable Appl., 10(4):1–21, 2019.

[205] Yuhong Li, Kun Ouyang, Nanxuan Li, Rahim Rahmani, Haojun Yang, and Yiwei Pei. A blockchain-assisted intelligent transportation system promoting data services with privacy protection. Sensors, 20(9):2483, 2020.

[206] Liviu-Adrian Hîrţan, Ciprian Dobre, and Horacio González-Vélez. Blockchain-based reputation for intelligent transportation systems. Sensors, 20(3):791, 2020.

[207] Md Sadek Ferdous, Mohammad Jabed Morshed Chowdhury, Kamanashis Biswas, Niaz Chowdhury, and Vallipuram Muthukkumarasamy. Immutable autobiography of smart cars leveraging blockchain technology. Knowledge Engineering Review, pages In–Press, 2019.

[208] Nisha Malik, Priyadarsi Nanda, Xiangjian He, and Ren Ping Liu. Vehicular networks with security and trust management solutions: proposed secured message exchange via blockchain technology. Wireless Networks, pages 1–20, 2020.

[209] Maher Salem. Blockchain-based authentication approach for securing transportation system. In International Symposium on Intelligent Computing Systems, pages 55–64. Springer, 2020.

[210] Di Wang and Xiaohong Zhang. Secure data sharing and customized services for intelligent transportation based on a consortium blockchain. IEEE Access, 8:56045–56059, 2020.

[211] Junho Lee, Jangwon Lee, and Hyungweon Park. A privacy preserving blockchain-based reward solution for vehicular networks. In 2020 IEEE International Conference on Consumer Electronics (ICCE), pages 1–4. IEEE, 2020.

[212] Leila Benarous, Benamar Kadri, and Ahmed Bouridane. Blockchain-based privacy-aware pseudonym management framework for vehicular networks. Arabian Journal for Science and Engineering, pages 1–17, 2020.

[213] Sana Hafeez, M Rehman Shahid, Amer Sohail, Sohail Jabbar, M Suleman, and Madiha Zafar. Blockchain based competent consensus algorithm for secure authentication in vehicular networks. In 2020 3rd International Conference on Computing, Mathematics and Engineering Technologies (iCoMET), pages 1–6. IEEE, 2020.

[214] Danda B Rawat, Ronald Doku, Abdulhamid Adebayo, Chandra Bajracharya, and Charles Kamhoua. Blockchain enabled named data networking for secure vehicle-to-everything communications. IEEE Network, 2020.

[215] Hong Liu, Pengfei Zhang, Geguang Pu, Tao Yang, Sabita Maharjan, and Yan Zhang. Blockchain empowered cooperative authentication with data traceability in vehicular edge computing. IEEE Transactions on Vehicular Technology, 69(4):4221–4232, 2020.

[216] Yongfeng Qian, Yingying Jiang, Long Hu, M Shamim Hossain, Mubarak Alrashoud, and Muneer Al-Hammadi. Blockchain-based privacy-aware

content caching in cognitive internet of vehicles. IEEE Network, 34(2):46–51, 2020.

[217] A Mohan Krishna and Amit Kumar Tyagi. Intrusion detection in intelligent transportation system and its applications using blockchain technology. In 2020 International Conference on Emerging Trends in Information Technology and Engineering (ic-ETITE), pages 1–8. IEEE, 2020.

[218] Lei Zhao and Tianhan Gao. Combination of pseudonym changing with blockchain-based data credibility for verifying accuracy of latest vehicle information in vanets. In International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing, pages 485–493. Springer, 2021.

[219] A.M. Eltahlawy and M.A. Azer. Using blockchain technology for the internet of vehicles. pages 54–61, 2021.

[220] G. Wei and Y. Ma. Privacy protection strategy of vehicle-to-grid network based on consortium blockchain and attribute-based signature. volume 661, 2021.

[221] T. Zhou, J. Shen, Y. Ren, and S. Ji. Threshold key management scheme for blockchain-based intelligent transportation systems. 2021, 2021.

[222] P. Lv, X. Zhang, J. Liu, T. Wei, and J. Xu. Blockchain oracle-based privacy preservation and reliable identification for vehicles. 12939 LNCS:512–520, 2021.

[223] J. Chen, K. Li, and P.S. Yu. Privacy-preserving deep learning model for decentralized vanets using fully homomorphic encryption and blockchain. 2021.

[224] Viktor Valaštín, Kritian Košt'ál, Rastislav Bencel, and Ivan Kotuliak. Blockchain based car-sharing platform. In 2019 International Symposium ELMAR, pages 5–8. IEEE, 2019.

[225] K. O. . Obour Agyekum, Q. Xia, E. Boateng Sifah, S. Amofa, K. Nketia Acheampong, J. Gao, R. Chen, H. Xia, J. C. Gee, X. Du, and M. Guizani. V-chain: A blockchain-based car lease platform. In 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), pages 1317–1325, 2018.

[226] G. M. Gandhi and Salvi. Artificial intelligence integrated blockchain for training autonomous cars. In 2019 Fifth International Conference on Science Technology Engineering and Mathematics (ICONSTEM), volume 1, pages 157–161, 2019.

[227] Mohammad Z Masoud, Yousef Jaradat, Ismael Jannoud, and Dema Zaidan. Carchain: A novel public blockchain-based used motor vehicle history reporting system. In 2019 IEEE Jordan International Joint Conference on Electrical Engineering and Information Technology (JEEIT), pages 683–688. IEEE, 2019.

[228] Bo Yin, Lishi Mei, Zexun Jiang, and Kai Wang. Joint cloud collaboration mechanism between vehicle clouds based on blockchain. In 2019 IEEE International Conference on Service-Oriented System Engineering (SOSE), pages 227–2275. IEEE, 2019.

[229] Junxing Zhang, Xumin Huang, Weiquan Ni, Maoqiang Wu, and Rong Yu. Vesenchain: Leveraging consortium blockchain for secure and efficient vehicular crowdsensing. In 2019 Chinese Control Conference (CCC), pages 6339–6344. IEEE, 2019.

[230] Chen Chen, Tingting Xiao, Tie Qiu, Ning Lv, and Qingqi Pei. Smart-contract-based economical platooning in blockchain-enabled urban internet of vehicles. IEEE Transactions on Industrial Informatics, 16(6):4122–4133, 2019.

[231] Panagiota Georgia Saranti, Dimitra Chondrogianni, and Stylianos Karatzas. Autonomous vehicles and blockchain technology are shaping the future of transportation. In The 4th conference on sustainable urban mobility, pages 797–803. Springer, 2018.

[232] Saeed Asadi Bagloee, Madjid Tavana, Glenn Withers, Michael Patriksson, and Mohsen Asadi. Tradable mobility permit with bitcoin and ethereum–a blockchain application in transportation. Internet of Things, 8:100103, 2019.

[233] Siu-Yeung Cho, Ningyuan Chen, and Xiuping Hua. Developing a vehicle networking platform based on blockchain technology. In International Conference on Blockchain, pages 186–201. Springer, 2019.

[234] Chuangxin Guo, Xiaobo Huang, Chengzhi Zhu, Xueping Wang, and Xiu Cao. Distributed electric vehicle control model based on blockchain. IOP Conference Series: Materials Science and Engineering, 486:012046, 2019.

[235] S Shreyas Ramachandran, AK Veeraraghavan, Uvais Karni, and K Sivaraman. Development of flexible autonomous car system using machine learning and blockchain. In International Symposium of Information and Internet Technology, pages 63–72. Springer, 2018.

[236] Maria Nadia Postorino and Giuseppe ML Sarné. A preliminary study for an agent blockchain-based framework supporting dynamic car-pooling. In WOA, pages 65–70, 2019.

[237] Peng Ren, Jingjing Xu, Yi Wang, and Xiaofeng Ma. Research and implementation of car rental alliance based on block-chain and internet of vehicles. Journal of Applied Sciences, 6:10, 2019.

[238] Zain Abubaker, Muhammad Usman Gurmani, Tanzeela Sultana, Shahzad Rizwan, Muhammad Azeem, Muhammad Zohaib Iftikhar, and Nadeem Javaid. Decentralized mechanism for hiring the smart autonomous vehicles using blockchain. In International Conference on Broadband and Wireless Computing, Communication and Applications, pages 733–746. Springer, 2019.

[239] Yuchuan Fu, Fei Richard Yu, Changle Li, Tom H Luan, and Yao Zhang. Vehicular blockchain-based collective learning for connected and autonomous vehicles. IEEE Wireless Communications, 27(2):197–203, 2020.

[240] Vadim Davydov and Sergey Bezzateev. Accident detection in internet of vehicles using blockchain technology. In 2020 International Conference on Information Networking (ICOIN), pages 766–771. IEEE, 2020.

[241] Yanxing Song, Yuchuan Fu, F Richard Yu, and Li Zhou. Blockchain-enabled internet of vehicles with cooperative positioning: A deep neural network approach. IEEE Internet of Things Journal, 7(4):3485–3498, 2020.

[242] Saltanat Narbayeva, Timur Bakibayev, Kuanysh Abeshev, Irina Makarova, Ksenia Shubenkova, and Anton Pashkevich. Blockchain technology on the way of autonomous vehicles development. Transportation Research Procedia, 44:168–175, 2020.

[243] Quanyi Hu, Simon Fong, Peng Qin, Jingzhi Guo, Yong Zhang, Dan Xu, Yuanlan Chen, and Jerome Yen. Intelligent car parking system based on blockchain processing reengineering. In International Conference on e-Business Engineering, pages 265–273. Springer, 2019.

[244] Yishui Zhu, Feng Du, Bo Wu, and Zongtao Duan. A sharing platform of emergency cars based on blockchain environment. In International Conference on Frontier Computing, pages 199–209. Springer, 2019.

[245] Pranav Kumar Singh, Roshan Singh, Sunit Kumar Nandi, Kayhan Zrar Ghafoor, Danda B Rawat, and Sukumar Nandi. Blockchain-based adaptive trust management in internet of vehicles using smart contract. IEEE Transactions on Intelligent Transportation Systems, 2020.

[246] Zeinab Shahbazi and Yung-Cheol Byun. A framework of vehicular security and demand service prediction based on data analysis integrated with blockchain approach. Sensors, 21(10):3314, 2021.

[247] Shirshak Raja Maskey, Shahriar Badsha, Shamik Sengupta, and Ibrahim Khalil. Alicia: Applied intelligence in blockchain based vanet: Accident validation as a case study. Information Processing & Management, 58(3):102508, 2021.

[248] Debashis Das, Sourav Banerjee, Uttam Ghosh, Utpal Biswas, and Ali Kashif Bashir. A decentralized vehicle anti-theft system using blockchain and smart contracts. Peer-to-Peer Networking and Applications, pages 1–14, 2021.

[249] Nisha Malik, Priyadarsi Nanda, Xiangjian He, and Ren Ping Liu. Vehicular networks with security and trust management solutions: proposed secured message exchange via blockchain technology. Wireless Networks, 26(6):4207–4226, 2020.

[250] Bogdan Cristian Florea and Dragos Daniel Taralunga. Blockchain iot for smart electric vehicles battery management. Sustainability, 12(10):3984, 2020.

[251] Shuai Zhou and Tianhan Gao. Vanets road condition warning and vehicle incentive mechanism based on blockchain. In International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing, pages 40–49. Springer, 2021.

[252] Lelio Campanile, Mauro Iacono, Fiammetta Marulli, and Michele Mastroianni. Designing a gdpr compliant blockchain-based iov distributed information tracking system. Information Processing & Management, 58(3):102511, 2021.

[253] Abdelghani Bekrar, Abdessamad Ait El Cadi, Raca Todosijevic, and Joseph Sarkis. Digitalizing the closing-of-the-loop for supply chains: A transportation and blockchain perspective. Sustainability, 13(5):2895, 2021.

[254] Haoye Chai, Supeng Leng, Yijin Chen, and Ke Zhang. A hierarchical blockchain-enabled federated learning algorithm for knowledge sharing in internet of vehicles. IEEE Transactions on Intelligent Transportation Systems, 2020.

[255] Chenyue Zhang, Wenjia Li, Yuansheng Luo, and Yupeng Hu. Ait: An ai-enabled trust management system for vehicular networks using blockchain technology. IEEE Internet of Things Journal, 8(5):3157–3169, 2020.

[256] H. Chauhan, D. Kumar, D. Gupta, S. Gupta, and V. Verma. Blockchain and iot based vehicle tracking system for industry 4.0 applications. volume 1022. IOP Publishing Ltd, 2021.

[257] 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. pages 62–67. Institute of Electrical and Electronics Engineers Inc., 2021.

[258] H. Liu, Y. Zhou, Y. Zhang, and Y. Su. A rough set fuzzy logic algorithm for visual tracking of blockchain logistics transportation labels. 41(4):4965–4972, 2021.

[259] Jinyu Zhang, Honghui Zhao, Yumeng Yang, and Jiaqi Yan. Towards transparency and trustworthy: A used-car deposit platform based on blockchain. In 2019 IEEE 19th International Conference on Software Quality, Reliability and Security Companion (QRS-C), pages 46–50. IEEE, 2019.

[260] He Bai, Cangshuai Wu, Yuexiang Yang, Geming Xia, and Yue Jiang. A blockchain-based traffic conditions and driving behaviors warning scheme in the internet of vehicles. In 2019 IEEE 19th International Conference on Communication Technology (ICCT), pages 1160–1164. IEEE, 2019.

[261] Varun Deshpande, Laurent George, and Hakim Badis. Safe: A blockchain and secure element based framework for safeguarding smart vehicles. In 2019 12th IFIP Wireless and Mobile Networking Conference (WMNC), pages 181–188. IEEE, 2019.

[262] Yanxing Song, Richard Yu, Yuchuan Fu, Li Zhou, and Azzedine Boukerche. Multi-vehicle cooperative positioning correction framework based on vehicular blockchain. In Proceedings of the 9th ACM Symposium on Design and Analysis of Intelligent Vehicular Networks and Applications, pages 23–29, 2019.

[263] Fabian Knirsch, Andreas Unterweger, and Dominik Engel. Privacy-preserving blockchain-based electric vehicle charging with dynamic tariff decisions. Computer Science-Research and Development, 33(1-2):71–79, 2018.

[264] Xuelin Wang and Hankun Shi. Research on container transportation application based on blockchain technology. In Proceedings of the Asia-Pacific Conference on Intelligent Medical 2018 & International Conference on Transportation and Traffic Engineering 2018, pages 277–281, 2018.

[265] Xiaohong Zhang and Di Wang. Adaptive traffic signal control mechanism for intelligent transportation based on a consortium blockchain. IEEE Access, 7:97281–97295, 2019.

[266] SV Aswathy and KV Lakshmy. Bvd-a blockchain based vehicle database system. In International Symposium on Security in Computing and Communication, pages 220–230. Springer, 2018.

[267] R Ramaguru, M Sindhu, and M Sethumadhavan. Blockchain for the internet of vehicles. In International Conference on Advances in Computing and Data Sciences, pages 412–423. Springer, 2019.

[268] Zuobin Ying, Maode Ma, and Longyang Yi. Bavpm: Practical autonomous vehicle platoon management supported by blockchain technique. In 2019 4th International Conference on Intelligent Transportation Engineering (ICITE), pages 256–260. IEEE, 2019.

[269] Anik Islam and Soo Young Shin. A blockchain-based secure healthcare scheme with the assistance of unmanned aerial vehicle in internet of things. Computers & Electrical Engineering, 84:106627, 2020.

[270] Sarah Iqbal, Asad Waqar Malik, Anis Ur Rahman, and Rafidah Md Noor. Blockchain-based reputation management for task offloading in micro-level vehicular fog network. IEEE Access, 8:52968–52980, 2020.

[271] Yueyue Dai, Du Xu, Ke Zhang, Sabita Maharjan, and Yan Zhang. Deep reinforcement learning and permissioned blockchain for content caching in vehicular edge computing and networks. IEEE Transactions on Vehicular Technology, 69(4):4312–4324, 2020.

[272] Xumin Huang, Dongdong Ye, Rong Yu, and Lei Shu. Securing parked vehicle assisted fog computing with blockchain and optimal smart contract design. IEEE/CAA Journal of Automatica Sinica, 7(2):426–441, 2020.

[273] Vasiliy Elagin, Anastasia Spirkina, Mikhail Buinevich, and Andrei Vladyko. Technological aspects of blockchain application for vehicle-to-network. Information, 11(10):465, 2020.

[274] Changle Li, Yuchuan Fu, Fei Richard Yu, Tom H Luan, and Yao Zhang. Vehicle position correction: A vehicular blockchain networks-based gps error sharing framework. IEEE Transactions on Intelligent Transportation Systems, 22(2):898–912, 2020.

[275] Jianfeng Ma, Tao Li, Jie Cui, Zuobin Ying, and Jiujun Cheng. Attribute-based secure announcement sharing among vehicles using blockchain. IEEE Internet of Things Journal, 2021.

[276] Myeonghyun Kim, Joonyoung Lee, Kisung Park, Yohan Park, Kil Houm Park, and Youngho Park. Design of secure decentralized car-sharing system using blockchain. IEEE Access, 9:54796–54810, 2021.

[277] R.S. Kaurav, R.R. Rout, and S. Vemireddy. Blockchain for emergency vehicle routing in healthcare services: An integrated secure and trustworthy system. pages 623–628. Institute of Electrical and Electronics Engineers Inc., 2021.

[278] J. H.S and A. S. Reputation management in vehicular network using blockchain. 2021.

[279] 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. 2021.

[280] 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. 2021.

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

[282] Z. Zhou, L. Tan, and G. Xu. Blockchain and edge computing based vehicle-to-grid energy trading in energy internet. In 2018 2nd IEEE Conference on Energy Internet and Energy System Integration (EI2), pages 1–5, 2018.

[283] Z. Zhou, B. Wang, Y. Guo, and Y. Zhang. Blockchain and computational intelligence inspired incentive-compatible demand response in internet of electric vehicles. IEEE Transactions on Emerging Topics in Computational Intelligence, 3(3):205–216, 2019.

[284] M. Pustišek, A. Kos, and U. Sedlar. Blockchain based autonomous selection of electric vehicle charging station. In 2016 International Conference on Identification, Information and Knowledge in the Internet of Things (IIKI), pages 217–222, 2016.

[285] Christian Gorenflo, Lukasz Golab, and Srinivasan Keshav. Mitigating trust issues in electric vehicle charging using a blockchain. In Proceedings of the Tenth ACM International Conference on Future Energy Systems, pages 160–164, 2019.

[286] Haoli Sun, Song Hua, Ence Zhou, Bingfeng Pi, Jun Sun, and Kazuhiro Yamashita. Using ethereum blockchain in internet of things: A solution for electric vehicle battery refueling. In Shiping Chen, Harry Wang, and Liang-Jie Zhang, editors, Blockchain – ICBC 2018, pages 3–17, Cham, 2018. Springer International Publishing.

[287] Chao Liu, Kok Keong Chai, Eng Tseng Lau, and Yue Chen. Blockchain based energy trading model for electric vehicle charging schemes. In Peter Han Joo Chong, Boon-Chong Seet, Michael Chai, and Saeed Ur Rehman, editors, Smart Grid and Innovative Frontiers in Telecommunications, pages 64–72, Cham, 2018. Springer International Publishing.

[288] Subhasis Thakur and John G. Breslin. Electric vehicle charging queue management with blockchain. In Andrzej M.J. Skulimowski, Zhengguo Sheng, Sondès Khemiri-Kallel, Christophe Cérin, and Ching-Hsien Hsu, editors, Internet of Vehicles. Technologies and Services Towards Smart City, pages 249–264, Cham, 2018. Springer International Publishing.

[289] Alejandro Ranchal Pedrosa and Giovanni Pau. Chargeltup: On blockchain-based technologies for autonomous vehicles. In Proceedings of the 1st Workshop on Cryptocurrencies and Blockchains for Distributed Systems, pages 87–92, 2018.

[290] Felipe Condon Silva, Mohamed A Ahmed, José Manuel Martínez, and Young-Chon Kim. Design and implementation of a blockchain-based energy trading platform for electric vehicles in smart campus parking lots. Energies, 12(24):4814, 2019.

[291] Zhengtang Fu, Peiwu Dong, and Yanbing Ju. An intelligent electric vehicle charging system for new energy companies based on consortium blockchain. Journal of Cleaner Production, page 121219, 2020.

[292] Yuancheng Li and Baiji Hu. An iterative two-layer optimization charging and discharging trading scheme for electric vehicle using consortium blockchain. IEEE Transactions on Smart Grid, 11(3):2627–2637, 2019.

[293] Md Mainul Islam, Md Shahjalal, Moh Khalid Hasan, and Yeong Min Jang. Blockchain-based energy transaction model for electric vehicles in v2g network. In 2020 International Conference on Artificial Intelligence in Information and Communication (ICAIIC), pages 628–630. IEEE, 2020.

[294] Ifiok Anthony Umoren, Syeda SA Jaffary, Muhammad Zeeshan Shakir, Konstantinos Katzis, and Hamed Ahmadi. Blockchain-based energy trading in electric vehicle enabled microgrids. IEEE Consumer Electronics Magazine, 2020.

[295] Chao Liu, Kok Keong Chai, Xiaoshuai Zhang, Eng Tseng Lau, and Yue Chen. Adaptive blockchain-based electric vehicle participation scheme in smart grid platform. IEEE Access, 6:25657–25665, 2018.

[296] Zhengtang Fu, Peiwu Dong, and Yanbing Ju. An intelligent electric vehicle charging system for new energy companies based on consortium blockchain. Journal of Cleaner Production, 261:121219, 2020.

[297] Muhammad Umar Javed, Nadeem Javaid, Abdulaziz Aldegheishem, Nabil Alrajeh, Muhammad Tahir, and Muhammad Ramzan. Scheduling charging of electric vehicles in a secured manner by emphasizing cost minimization using blockchain technology and ipfs. Sustainability, 12(12):5151, 2020.

[298] Gang Sun, Miao Dai, Feng Zhang, Hongfang Yu, Xiaojiang Du, and Mohsen Guizani. Blockchain-enhanced high-confidence energy sharing in internet of electric vehicles. IEEE Internet of Things Journal, 7(9):7868–7882, 2020.

[299] Ifiok Anthony Umoren, Syeda Sanober Ali Jaffary, Muhammad Zeeshan Shakir, Konstantinos Katzis, and Hamed Ahmadi. Blockchain-based energy trading in electric-vehicle-enabled microgrids. IEEE Consumer Electronics Magazine, 9(6):66–71, 2020.

[300] Yangyang Long, Yuling Chen, Wei Ren, Hui Dou, and Neal Naixue Xiong. Depet: A decentralized privacy-preserving energy trading scheme for vehicular energy network via blockchain and k-anonymity. IEEE Access, 8:192587–192596, 2020.

[301] Zhaoxiong Huang, Zhenhao Li, Chun Sing Lai, Zhuoli Zhao, Xiaomei Wu, Xuecong Li, Ning Tong, and Loi Lei Lai. A novel power market mechanism based on blockchain for electric vehicle charging stations. Electronics, 10(3):307, 2021.

[302] Ayesha Sadiq, Muhammad Umar Javed, Rabiya Khalid, Ahmad Almogren, Muhammad Shafiq, and Nadeem Javaid. Blockchain based data and energy trading in internet of electric vehicles. IEEE Access, 2020.

[303] K. Sukkrajang, R. Duangsoithong, and K. Chalermyannont. Trade distance and price model for electric vehicle charging using blockchain-based technology. pages 964–967, 2021.

[304] 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 Systems, 12(2):285–355, 2021.

[305] J.C. Ferreira, C.F. da Silva, and J.P. Martins. Roaming service for electric vehicle charging using blockchain-based digital identity. 14(6), 2021.

[306] S.N. Gowda, B.A. Eraqi, H. Nazaripouya, and R. Gadh. Assessment and tracking electric vehicle battery degradation cost using blockchain. 2021.

[307] L.P. Qian, Y. Wu, X. Xu, B. Ji, Z. Shi, and W. Jia. Distributed charging-record management for electric vehicle networks via blockchain. 8(4):2150–2162, 2021.

[308] M. Baza, R. Amer, A. Rasheed, G. Srivastava, M. Mahmoud, and W. Alasmary. A blockchain-based energy trading scheme for electric vehicles. Institute of Electrical and Electronics Engineers Inc., 2021.

[309] N.A. Hayla, M.S. Abegaz, H.Y. Yasin, T.A. Ayall, G. Sun, and G. Liu. Consensus mechanism for blockchain-enabled vehicle-to-vehicle energy trading in the internet of electric vehicles. 2021.

[310] 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. 2021.

[311] 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 [ic]. 141(8):903–908, 2021.

[312] J. Zhao, C. He, C. Peng, and X. Zhang. Blockchain for effective renewable energy management in the intelligent transportation system. 2021.

[313] N. Zhao and H. Wu. Blockchain combined with smart contract to keep safety energy trading for autonomous vehicles. In 2019 IEEE 89th Vehicular Technology Conference (VTC2019-Spring), pages 1–5, 2019.

[314] Shiyuan Xu, Xue Chen, and Yunhua He. Evchain: An anonymous blockchain-based system for charging-connected electric vehicles. Tsinghua Science and Technology, 26(6):845–856, 2021.

[315] M. Aloqaily, I.A. Ridhawi, and M. Guizani. Energy-aware blockchain and federated learning-supported vehicular networks. 2021.

[316] U. Asfia, V. Kamuni, A. Sheikh, S. Wagh, and D. Patel. Energy trading of electric vehicles using blockchain and smart contracts. In 2019 18th European Control Conference (ECC), pages 3958–3963, 2019.

[317] Z. Su, Y. Wang, Q. Xu, M. Fei, Y. Tian, and N. Zhang. A secure charging scheme for electric vehicles with smart communities in energy blockchain. IEEE Internet of Things Journal, 6(3):4601–4613, 2019.

[318] 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, 7:160546–160558, 2019.

[319] Yuntao Wang, Zhou Su, and Ning Zhang. Bsis: Blockchain-based secure incentive scheme for energy delivery in vehicular energy network. IEEE Transactions on Industrial Informatics, 15(6):3620–3631, 2019.

[320] MyeongHyun Kim, KiSung Park, SungJin Yu, JoonYoung Lee, YoungHo Park, Sang-Woo Lee, and BoHeung Chung. A secure charging system for electric vehicles based on blockchain. Sensors, 19(13):3028, 2019.

[321] Zhenyu Zhou, Bingchen Wang, Mianxiong Dong, and Kaoru Ota. Secure and efficient vehicle-to-grid energy trading in cyber physical systems: Integration of blockchain and edge computing. IEEE Transactions on Systems, Man, and Cybernetics: Systems, 50(1):43–57, 2019.

[322] Xi Chen, Tianyang Zhang, Wenxing Ye, Zhiwei Wang, and Herbert Ho-Ching Iu. Blockchain-based electric vehicle incentive system for renewable energy consumption. IEEE Transactions on Circuits and Systems II: Express Briefs, 68(1):396–400, 2020.

[323] S Velliangiri, G Krishna Lava Kumar, and P Karthikeyan. Unsupervised blockchain for safeguarding confidential information in vehicle assets transfer. In 2020 6th International Conference on Advanced Computing and Communication Systems (ICACCS), pages 44–49. IEEE, 2020.

[324] Mumin Cebe, Enes Erdin, Kemal Akkaya, Hidayet Aksu, and Selcuk Uluagac. Block4forensic: An integrated lightweight blockchain framework for forensics applications of connected vehicles. IEEE Communications Magazine, 56(10):50–57, 2018.

[325] Kei Leo Brousmiche, Thomas Heno, Christian Poulain, Antoine Dalmieres, and Elyes Ben Hamida. Digitizing, securing and sharing vehicles life-cycle over a consortium blockchain: Lessons learned. In 2018 9th IFIP international conference on new technologies, mobility and security (NTMS), pages 1–5. IEEE, 2018.

[326] Tigang Jiang, Hua Fang, and Honggang Wang. Blockchain-based internet of vehicles: Distributed network architecture and performance analysis. IEEE Internet of Things Journal, 6(3):4640–4649, 2018.

[327] Kei Leo Brousmiche, Antoine Durand, Thomas Heno, Christian Poulain, Antoine Dalmieres, and Elyes Ben Hamida. Hybrid cryptographic protocol for secure vehicle data sharing over a consortium blockchain. In 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), pages 1281–1286. IEEE, 2018.

[328] Xiaohong Zhang and Xiaofeng Chen. Data security sharing and storage based on a consortium blockchain in a vehicular ad-hoc network. IEEE Access, 7:58241–58254, 2019.

[329] Kang Liu, Wuhui Chen, Zibin Zheng, Zhenni Li, and Wei Liang. A novel debt-credit mechanism for blockchain-based data-trading in internet of vehicles. IEEE Internet of Things Journal, 6(5):9098–9111, 2019.

[330] Shihan Bao, Yue Cao, Ao Lei, Philip Asuquo, Haitham Cruickshank, Zhili Sun, and Michael Huth. Pseudonym management through blockchain: Cost-efficient privacy preservation on intelligent transportation systems. IEEE Access, 7:80390–80403, 2019.

[331] Francesco Morano, Claudio Ferretti, Alberto Leporati, Paolo Napoletano, and Raimondo Schettini. A blockchain technology for protection and probative value preservation of vehicle driver data. In 2019 IEEE 23rd International Symposium on Consumer Technologies (ISCT), pages 167–172. IEEE, 2019.

[332] Rohit Sharma and Suchetana Chakraborty. B2vdm: Blockchain based vehicular data management. In 2018 International Conference on Advances in Computing, Communications and Informatics (ICACCI), pages 2337–2343. IEEE, 2018.

[333] Farah Kandah, Brennan Huber, Amani Altarawneh, Sai Medury, and Anthony Skjellum. Blast: Blockchain-based trust management in smart cities and connected vehicles setup. In 2019 IEEE High Performance Extreme Computing Conference (HPEC), pages 1–7. IEEE, 2019.

[334] Sachin Sharma, Kamal Kumar Ghanshala, and Seshadri Mohan. Blockchain-based internet of vehicles (iov): An efficient secure ad hoc vehicular networking architecture. In 2019 IEEE 2nd 5G World Forum (5GWF), pages 452–457. IEEE, 2019.

[335] Shihan Bao, Ao Lei, Haitham Cruickshank, Zhili Sun, Philip Asuquo, and Waleed Hathal. A pseudonym certificate management scheme based on blockchain for internet of vehicles. In 2019 IEEE Intl Conf on Dependable, Autonomic and Secure Computing, Intl Conf on

Pervasive Intelligence and Computing, Intl Conf on Cloud and Big Data Computing, Intl Conf on Cyber Science and Technology Congress (DASC/PiCom/CBDCom/CyberSciTech), pages 28–35. IEEE, 2019.

[336] Chuan Chen, Jiajing Wu, Hui Lin, Wuhui Chen, and Zibin Zheng. A secure and efficient blockchain-based data trading approach for internet of vehicles. IEEE Transactions on Vehicular Technology, 68(9):9110–9121, 2019.

[337] Mohamed Baza, Mahmoud Nabil, Noureddine Lasla, Kemal Fidan, Mohamed Mahmoud, and Mohamed Abdallah. Blockchain-based firmware update scheme tailored for autonomous vehicles. In 2019 IEEE Wireless Communications and Networking Conference (WCNC), pages 1–7. IEEE, 2019.

[338] Hao Guo, Ehsan Meamari, and Chien-Chung Shen. Blockchain-inspired event recording system for autonomous vehicles. In 2018 1st IEEE International Conference on Hot Information-Centric Networking (HotICN), pages 218–222. IEEE, 2018.

[339] Mehmet Demir, Ozgur Turetken, and Alexander Ferworn. Blockchain based transparent vehicle insurance management. In 2019 Sixth International Conference on Software Defined Systems (SDS), pages 213–220. IEEE, 2019.

[340] Md Abdur Rahman, Md Mamunur Rashid, Stuart J Barnes, and Syed Maruf Abdullah. A blockchain-based secure internet of vehicles management framework. In 2019 UK/China Emerging Technologies (UCET), pages 1–4. IEEE, 2019.

[341] Lei Zhang, Mingxing Luo, Jiangtao Li, Man Ho Au, Kim-Kwang Raymond Choo, Tong Chen, and Shengwei Tian. Blockchain based secure data sharing system for internet of vehicles: A position paper. Vehicular Communications, 16:85–93, 2019.

[342] Liudmila Zavolokina, Florian Spychiger, Claudio Tessone, and Gerhard Schwabe. Incentivizing data quality in blockchains for inter-organizational networks–learning from the digital car dossier. In International Conference of Information Systems (ICIS 2018), San Francisco, USA, 12-16 December 2018. University of Zurich, 2018.

[343] David Holtkemper and Simon Wieninger. Company data in the blockchain: A juxtaposition of technological drivers and potential applications. In 2018 Portland International Conference on Management of Engineering and Technology (PICMET), pages 1–7. IEEE, 2018.

[344] Qifan Wang, Lei Zhou, Zhe Tang, and Guojun Wang. A consortium blockchain-based model for data sharing in internet of vehicles. In International Conference on Smart City and Informatization, pages 253–267. Springer, 2019.

[345] Kexin Shi, Liehuang Zhu, Can Zhang, Lei Xu, and Feng Gao. Blockchain-based multimedia sharing in vehicular social networks with privacy protection. Multimedia Tools and Applications, pages 1–21, 2020.

[346] Muhammad Umar Javed, Mubariz Rehman, Nadeem Javaid, Abdulaziz Aldegheishem, Nabil Alrajeh, and Muhammad Tahir. Blockchain-based secure data storage for distributed vehicular networks. Applied Sciences, 10(6):2011, 2020.

[347] Chen Chen, Cong Wang, Tie Qiu, Ning Lv, and Qingqi Pei. A secure content sharing scheme based on blockchain in vehicular named data networks. IEEE Transactions on Industrial Informatics, 16(5):3278–3289, 2019.

[348] Yunlong Lu, Xiaohong Huang, Ke Zhang, Sabita Maharjan, and Yan Zhang. Blockchain empowered asynchronous federated learning for secure data sharing in internet of vehicles. IEEE Transactions on Vehicular Technology, 69(4):4298–4311, 2020.

[349] Yunlong Lu, Xiaohong Huang, Ke Zhang, Sabita Maharjan, and Yan Zhang. Blockchain empowered asynchronous federated learning for secure data sharing in internet of vehicles. IEEE Transactions on Vehicular Technology, 69(4):4298–4311, 2020.

[350] Zhou Su, Yuntao Wang, Qichao Xu, and Ning Zhang. Lvbs: Lightweight vehicular blockchain for secure data sharing in disaster rescue. IEEE Transactions on Dependable and Secure Computing, 2020.

[351] Muhammad Umar Javed, Mubariz Rehman, Nadeem Javaid, Abdulaziz Aldegheishem, Nabil Alrajeh, and Muhammad Tahir. Blockchain-based secure data storage for distributed vehicular networks. Applied Sciences, 10(6):2011, 2020.

[352] Hui Li, Lishuang Pei, Dan Liao, Song Chen, Ming Zhang, and Du Xu. Fadb: A fine-grained access control scheme for vanet data based on blockchain. IEEE Access, 8:85190–85203, 2020.

[353] Meng Shen, Jie Zhang, Liehuang Zhu, Ke Xu, and Xiangyun Tang. Secure svm training over vertically-partitioned datasets using consortium blockchain for vehicular social networks. IEEE Transactions on Vehicular Technology, 69(6):5773–5783, 2019.

[354] Chen Chen, Cong Wang, Tie Qiu, Ning Lv, and Qingqi Pei. A secure content sharing scheme based on blockchain in vehicular named data networks. IEEE Transactions on Industrial Informatics, 16(5):3278–3289, 2019.

[355] Seema Verma et al. A blockchain-based secure car hiring system. In Cyber Security and Digital Forensics, pages 341–349. Springer, 2022.

[356] Mohamed Haouari, Mariem Mhiri, Mazen El-Masri, and Karim Al-Yafi. A novel proof of useful work for a blockchain storing transportation transactions. Information Processing & Management, 59(1):102749, 2022.

[357] D. Huang, Z.-Y. Tang, W.-Y. Hu, and Q.-Z. Wu. Blockchain-based electric vehicle charging reputation management mechanism. pages 58–61, 2021.

[358] Yueyue Dai, Du Xu, Ke Zhang, Sabita Maharjan, and Yan Zhang. Deep reinforcement learning and permissioned blockchain for content caching in vehicular edge computing and networks. IEEE Transactions on Vehicular Technology, 69(4):4312–4324, 2020.

[359] Kai Fan, Qiang Pan, Kuan Zhang, Yuhan Bai, Shili Sun, Hui Li, and Yintang Yang. A secure and verifiable data sharing scheme based on blockchain in vehicular social networks. IEEE Transactions on Vehicular Technology, 69(6):5826–5835, 2020.

[360] Chuka Oham, Regio A Michelin, Raja Jurdak, Salil S Kanhere, and Sanjay Jha. B-ferl: Blockchain based framework for securing smart vehicles. Information Processing & Management, 58(1):102426, 2021.

[361] Khizar Abbas, Lo'Ai A Tawalbeh, Ahsan Rafiq, Ammar Muthanna, Ibrahim A Elgendy, Abd El-Latif, and A Ahmed. Convergence of blockchain and iot for secure transportation systems in smart cities. Security and Communication Networks, 2021, 2021.

[362] Z. Shahbazi and Y.-C. Byun. A framework of vehicular security and demand service prediction based on data analysis integrated with blockchain approach. Sensors, 21(10), 2021.

[363] 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)/Journal of Zhejiang University (Engineering Science), 55(5):957–965, 2021.

[364] Y. Yin, Y. Li, B. Ye, T. Liang, and Y. Li. A blockchain-based incremental update supported data storage system for intelligent vehicles. IEEE Transactions on Vehicular Technology, 70(5):4880–4893, 2021.

[365] S. Distefano, A.D. Giacomo, and M. Mazzara. Trustworthiness for transportation ecosystems: The blockchain vehicle information system. 22(4):2013–2022, 2021.

[366] 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. 8(4):2087–2101, 2021.

[367] Y. Zou, F. Shen, F. Yan, J. Lin, and Y. Qiu. Reputation-based regional federated learning for knowledge trading in blockchain-enhanced iov. volume 2021-March. Institute of Electrical and Electronics Engineers Inc., 2021.

[368] 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. 2021.

[369] D. Chulerttiyawong and A. Jamalipour. A blockchain assisted vehicular pseudonym issuance and management system for conditional privacy enhancement. 9:127305–127319, 2021.

[370] 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. 2021.

[371] B. Ghimire and D.B. Rawat. Secure, privacy preserving and verifiable federating learning using blockchain for internet of vehicles. 2021.

[372] S.K. Singh, P.K. Sharma, Y. Pan, and J.H. Park. Biiovt: Blockchain-based secure storage architecture for intelligent internet of vehicular things. 2021.

[373] J. Cui, F. Ouyang, Z. Ying, L. Wei, and H. Zhong. Secure and efficient data sharing among vehicles based on consortium blockchain. 2021.

[374] Ning Zhao, Hao Wu, and Xiaonan Zhao. Consortium blockchain-based secure software defined vehicular network. Mobile Networks and Applications, 25(1):314–327, 2020.

[375] Sowmya Kudva, Shahriar Badsha, Shamik Sengupta, Hung La, Ibrahim Khalil, and Mohammed Atiquzzaman. A scalable blockchain based trust management in vanet routing protocol. Journal of Parallel and Distributed Computing, 152:144–156, 2021.

[376] Yanli Ren, Xiangyu Li, Shi-Feng Sun, Xingliang Yuan, and Xinpeng Zhang. Privacy-preserving batch verification signature scheme based on blockchain for vehicular ad-hoc networks. Journal of Information Security and Applications, 58:102698, 2021.

[377] Lijun Sun, Qian Yang, Xiao Chen, and Zhenxiang Chen. Rc-chain: Reputation-based crowdsourcing blockchain for vehicular networks. Journal of Network and Computer Applications, 176:102956, 2021.

[378] Sarah Iqbal, Asad Waqar Malik, Anis Ur Rahman, and Rafidah Md Noor. Blockchain-based reputation management for task offloading in micro-level vehicular fog network. IEEE Access, 8:52968–52980, 2020.

[379] 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. 8(4):2395–2408, 2021.

[380] D. Zhang, F.R. Yu, and R. Yang. Blockchain-based multi-access edge computing for future vehicular networks: A deep compressed neural network approach. 2021.

[381] 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. 2021.

[382] 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. 2021.

[383] Madhusudan Singh and Shiho Kim. Trust bit: Reward-based intelligent vehicle commination using blockchain paper. In 2018 IEEE 4th World Forum on Internet of Things (WF-IoT), pages 62–67. IEEE, 2018.

[384] Madhusudan Singh and Shiho Kim. Introduce reward-based intelligent vehicles communication using blockchain. In 2017 International SoC Design Conference (ISOCC), pages 15–16. IEEE, 2017.

[385] Alviansyah Arman Yusuf, Dwi Kurnia Basuki, Sritrusta Sukaridhoto, Yogi Putra Pratama, Fariz Bramasta Putra, and Heri Yulianus. Armchain-a blockchain based sensor data communication for the vehicle as a mobile sensor network. In 2019 International Electronics Symposium (IES), pages 539–543. IEEE, 2019.

[386] Jose Angel Leon Calvo and Rudolf Mathar. Secure blockchain-based communication scheme for connected vehicles. In 2018 European Conference on Networks and Communications (EuCNC), pages 347–351. IEEE, 2018.

[387] Haoye Chai, Supeng Leng, Ming Zeng, and Haoyang Liang. A hierarchical blockchain aided proactive caching scheme for internet of vehicles. In ICC 2019-2019 IEEE International Conference on Communications (ICC), pages 1–6. IEEE, 2019.

[388] Alexander Kuzmin and Evgeny Znak. Blockchain-base structures for a secure and operate network of semi-autonomous unmanned aerial vehicles. In 2018 IEEE International Conference on Service Operations and Logistics, and Informatics (SOLI), pages 32–37. IEEE, 2018.

[389] Farhan Ahmad, Chaker Abdelaziz Kerrache, Fatih Kurugollu, and Rasheed Hussain. Realization of blockchain in named data networking-based internet-of-vehicles. IT Professional, 21(4):41–47, 2019.

[390] AS Kulathunge and HROE Dayarathna. Communication framework for vehicular ad-hoc networks using blockchain: Case study of metro manila electric shuttle automation project. In 2019 International Research Conference on Smart Computing and Systems Engineering (SCSE), pages 85–90. IEEE, 2019.

[391] Wei Hu, Yawei Hu, Wenhui Yao, and Huanhao Li. A blockchain-based byzantine consensus algorithm for information authentication of the internet of vehicles. IEEE Access, 7:139703–139711, 2019.

[392] Arkil Patel, Naigam Shah, Trupil Limbasiya, and Debasis Das. Vehiclechain: Blockchain-based vehicular data transmission scheme for smart city. In 2019 IEEE International Conference on Systems, Man and Cybernetics (SMC), pages 661–667. IEEE, 2019.

[393] Paulo C Bartolomeu and Joaquim Ferreira. Blockchain enabled vehicular communications: Fad or future? In 2018 IEEE 88th Vehicular Technology Conference (VTC-Fall), pages 1–5. IEEE, 2018.

[394] Benjamin Leiding, Parisa Memarmoshrefi, and Dieter Hogrefe. Self-managed and blockchain-based vehicular ad-hoc networks. In Proceedings of the 2016 ACM International Joint Conference on Pervasive and Ubiquitous Computing: Adjunct, pages 137–140, 2016.

[395] Argyris Gkogkidis, Nikolaos Giachoudis, Georgios Spathoulas, and Ioannis Anagnostopoulos. Implementing a blockchain infrastructure on top of vehicular ad hoc networks. In The 4th Conference on Sustainable Urban Mobility, pages 764–771. Springer, 2018.

[396] Madhusudan Singh and Shiho Kim. Branch based blockchain technology in intelligent vehicle. Computer Networks, 145:219–231, 2018.

[397] Ao Lei, Yue Cao, Shihan Bao, Dasen Li, Philip Asuquo, Haitham Cruickshank, and Zhili Sun. A blockchain based certificate revocation scheme for vehicular communication systems. Future Generation Computer Systems, 110:892–903, 2020.

[398] Jing Wu, Xin Cui, Wei Hu, Keke Gai, Xing Liu, Kai Zhang, and Kai Xu. A new sustainable interchain design on transport layer for blockchain. In International Conference on Smart Blockchain, pages 12–21. Springer, 2018.

[399] Alessio Bonadio, Francesco Chiti, Romano Fantacci, and Vincenzo Vespri. An integrated framework for blockchain inspired fog communications and computing in internet of vehicles. Journal of Ambient Intelligence and Humanized Computing, 11(2):755–762, 2020.

[400] Muhammd Awais Hassan, Ume Habiba, Usman Ghani, and Muhmmad Shoaib. A secure message-passing framework for inter-vehicular communication using blockchain. International Journal of Distributed Sensor Networks, 15(2):1550147719829677, 2019.

[401] Lewis Nkenyereye, Bayu Adhi Tama, Muhammad K Shahzad, and Yoon-Ho Choi. Secure and blockchain-based emergency driven message protocol for 5g enabled vehicular edge computing. Sensors, 20(1):154, 2020.

[402] Vidya Krishnan M, Rajesh Koduri, Sivaprasad Nandyala, and Mithun Manalikandy. Secure vehicular communication using blockchain technology. Technical report, SAE Technical Paper, 2020.

[403] Lucas R Abbade, Filipe M Ribeiro, Matheus H da Silva, Alisson FP Morais, Everton S de Morais, Estevan M Lopes, Antonio M Alberti, and Joel JPC Rodrigues. Blockchain applied to vehicular odometers. IEEE Network, 34(1):62–68, 2020.

[404] Priya Singh, Pooja Khanna, and Sachin Kumar. Communication architecture for vehicular ad hoc networks, with blockchain security. In 2020 International Conference on Computation, Automation and Knowledge Management (ICCAKM), pages 68–72. IEEE, 2020.

[405] Amritesh Kumar, Amrendra Singh Yadav, and Dharmender Singh Kushwaha. Vchain: Efficient blockchain based vehicular communication protocol. In 2020 10th International Conference on Cloud Computing, Data Science & Engineering (Confluence), pages 762–768. IEEE, 2020.

[406] Hakima Khelifi, Senlin Luo, Boubakr Nour, Hassine Moungla, Syed Hassan Ahmed, and Mohsen Guizani. A blockchain-based architecture for secure vehicular named data networks. Computers & Electrical Engineering, 86:106715, 2020.

[407] Danda B Rawat, Ronald Doku, Abdulhamid Adebayo, Chandra Bajracharya, and Charles Kamhoua. Blockchain enabled named data networking for secure vehicle-to-everything communications. IEEE Network, 34(5):185–189, 2020.

[408] Ao Lei, Yue Cao, Shihan Bao, Dasen Li, Philip Asuquo, Haitham Cruickshank, and Zhili Sun. A blockchain based certificate revocation scheme for vehicular communication systems. Future Generation Computer Systems, 110:892–903, 2020.

[409] Zehui Zheng, Jianping Pan, and Lin Cai. Lightweight blockchain consensus protocols for vehicular social networks. IEEE Transactions on Vehicular Technology, 69(6):5736–5748, 2020.

[410] AFM Akhter, Mohiuddin Ahmed, AFM Shah, Adnan Anwar, ASM Kayes, and Ahmet Zengin. A blockchain-based authentication protocol for cooperative vehicular ad hoc network. Sensors, 21(4):1273, 2021.

[411] Palak Bagga, Anil Kumar Sutrala, Ashok Kumar Das, and Pandi Vijayakumar. Blockchain-based batch authentication protocol for internet of vehicles. Journal of Systems Architecture, 113:101877, 2021.

[412] Yonggang Xiao, Yanbing Liu, and Tun Li. Edge computing and blockchain for quick fake news detection in iov. Sensors, 20(16):4360, 2020.

[413] Rajesh Gupta, Aparna Kumari, and Sudeep Tanwar. A taxonomy of blockchain envisioned edge-as-a-connected autonomous vehicles. Transactions on Emerging Telecommunications Technologies, 32(6):e4009, 2021.

[414] Y. Jiang, X. Shen, and S. Zheng. An effective data sharing scheme based on blockchain in vehicular social networks. 10(2):1–17, 2021.

[415] Haijun Liao, Yansong Mu, Zhenyu Zhou, Meng Sun, Zhao Wang, and Chao Pan. Blockchain and learning-based secure and intelligent task offloading for vehicular fog computing. IEEE Transactions on Intelligent Transportation Systems, 2020.

[416] Zisang Xu, Wei Liang, Kuan-Ching Li, Jianbo Xu, and Hai Jin. A blockchain-based roadside unit-assisted authentication and key agreement protocol for internet of vehicles. Journal of Parallel and Distributed Computing, 149:29–39, 2021.

[417] Sowmya Kudva, Shahriar Badsha, Shamik Sengupta, Ibrahim Khalil, and Albert Zomaya. Towards secure and practical consensus for blockchain based vanet. Information Sciences, 545:170–187, 2021.

[418] Muhammad Firdaus and Kyung-Hyune Rhee. On blockchain-enhanced secure data storage and sharing in vehicular edge computing networks. Applied Sciences, 11(1):414, 2021.

[419] Mohsin Kamal, Gautam Srivastava, and Muhammad Tariq. Blockchain-based lightweight and secured v2v communication in the internet of vehicles. IEEE Transactions on Intelligent Transportation Systems, 2020.

[420] Anusha Vangala, Basudeb Bera, Sourav Saha, Ashok Kumar Das, Neeraj Kumar, and Young Ho Park. Blockchain-enabled certificate-based authentication for vehicle accident detection and notification in intelligent transportation systems. IEEE Sensors Journal, 2020.

[421] Qinglei Kong, Le Su, and Maode Ma. Achieving privacy-preserving and verifiable data sharing in vehicular fog with blockchain. IEEE Transactions on Intelligent Transportation Systems, 2020.

[422] Siming Wang, Dongdong Ye, Xumin Huang, Rong Yu, Yongjian Wang, and Yan Zhang. Consortium blockchain for secure resource sharing in vehicular edge computing: A contract-based approach. IEEE Transactions on Network Science and Engineering, 2020.

[423] Shupeng Wang, Shouming Sun, Xiaojie Wang, Zhaolong Ning, and Joel JPC Rodrigues. Secure crowdsensing in 5g internet of vehicles: When deep reinforcement learning meets blockchain. IEEE Consumer Electronics Magazine, 2020.

[424] Mahadev Gawas, Hemprasad Patil, and Sweta S Govekar. An integrative approach for secure data sharing in vehicular edge computing using blockchain. Peer-to-Peer Networking and Applications, pages 1–19, 2021.

[425] Xiao Zheng, Mingchu Li, Yuanfang Chen, Jun Guo, Muhammad Alam, and Weitong Hu. Blockchain-based secure computation offloading in vehicular networks. IEEE Transactions on Intelligent Transportation Systems, 2020.

[426] Maha Kadadha and Hadi Otrok. A blockchain-enabled relay selection for qos-olsr in urban vanet: A stackelberg game model. Ad Hoc Networks, 117:102502, 2021.

[427] S. Kudva, S. Badsha, S. Sengupta, H. La, I. Khalil, and M. Atiquzzaman. A scalable blockchain based trust management in vanet routing protocol. Journal of Parallel and Distributed Computing, 152:144–156, 2021.

[428] B. Li, R. Liang, D. Zhu, W. Chen, and Q. Lin. Blockchain-based trust management model for location privacy preserving in vanet. IEEE Transactions on Intelligent Transportation Systems, 22(6):3765–3775, 2021.

[429] E.-H. Diallo, O. Dib, N.R. Zema, and K. Al Agha. When proof-of-work (pow) based blockchain meets vanet environments. pages 336–343, 2021.

[430] M. Zang, Y. Zhu, R. Lan, Y. Liu, and X. Luo. Bavc: Efficient blockchain-based authentication scheme for vehicular secure communication. pages 346–350, 2021.

[431] K.H. Chan, M. Pasco, and B.H.C. Cheng. Towards a blockchain framework for autonomous vehicle system integrity. SAE International Journal of Transportation Cybersecurity and Privacy, 4(1):19–38, 2021.

[432] H. Ye and S. Park. Reliable vehicle data storage using blockchain and ipfs. Electronics (Switzerland), 10(10), 2021.

[433] S. Islam, S. Badsha, S. Sengupta, H. La, I. Khalil, and M. Atiquzzaman. Blockchain-enabled intelligent vehicular edge computing. IEEE Network, 35(3):125–131, 2021.

[434] Y. Zhang, J. Misic, and Z. Zheng. Guest editorial introduction to the special section on blockchain for vehicles and intelligent communications. IEEE Transactions on Vehicular Technology, 70(5):3998–4000, 2021.

[435] U. Javaid and B. Sikdar. A secure and scalable framework for blockchain based edge computation offloading in social internet of vehicles. IEEE Transactions on Vehicular Technology, 70(5):4022–4036, 2021.

[436] C. Pu. A novel blockchain-based trust management scheme for vehicular networks. volume 2021-April, 2021.

[437] N. Khatri, R. Shrestha, and S.Y. Nam. Security issues with in-vehicle networks, and enhanced countermeasures based on blockchain. 10(8), 2021.

[438] M. Kong, J. Zhao, X. Sun, and Y. Nie. Secure and efficient computing resource management in blockchain-based vehicular fog computing. 18(4):115–125, 2021.

[439] A. Sarker, S. Byun, W. Fan, and S.-Y. Chang. Blockchain-based root of trust management in security credential management system for vehicular communications. pages 223–231, 2021.

[440] 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. 8(4):2468–2482, 2021.

[441] D. Moussaoui, B. Kadri, M. Feham, and B. Ammar Bensaber. A distributed blockchain based pki (bcpki) architecture to enhance privacy in vanet. pages 75–79, 2021.

[442] F. Dewanta and M. Mambo. Bpt scheme: Establishing trusted vehicular fog computing service for rural area based on blockchain approach. 70(2):1752–1769, 2021.

[443] 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. Institute of Electrical and Electronics Engineers Inc., 2021.

[444] S. More, R. Sonkamble, U. Naik, S. Phansalkar, P. More, and B.S. Saini. Secured communication in vehicular adhoc networks (vanets) using blockchain. volume 1022. IOP Publishing Ltd, 2021.

[445] C. Mao, K. Xie, L. Gao, M. Wan, and S. Liu. Design of internet of vehicles authentication scheme based on blockchain. volume 1738. IOP Publishing Ltd, 2021.

[446] S.-K. Kim. Enhanced iov security network by using blockchain governance game. 9(2):1–13, 2021.

[447] 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. 2021.

[448] Z. Zhou, M. Wang, J. Huang, S. Lin, and Z. Lv. Blockchain in big data security for intelligent transportation with 6g. 2021.

[449] D. Wang, L. Zhang, C. Huang, and X. Shen. A privacy-preserving trust management system based on blockchain for vehicular networks. volume 2021-March. Institute of Electrical and Electronics Engineers Inc., 2021.

[450] 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. 2021.

[451] 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. 278:406–416, 2021.

[452] 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. 278:142–151, 2021.

[453] V. Hassija, M. Zaid, G. Singh, A. Srivastava, and V. Saxena. Cryptober: A blockchain-based secure and cost-optimal car rental platform. In 2019 Twelfth International Conference on Contemporary Computing (IC3), pages 1–6, 2019.

[454] Chen Chen, Tingting Xiao, Tie Qiu, Ning Lv, and Qingqi Pei. Smart-contract-based economical platooning in blockchain-enabled urban internet of vehicles. IEEE Transactions on Industrial Informatics, 16(6):4122–4133, 2019.

[455] Faisal Jamil, Omar Cheikhrouhou, Harun Jamil, Anis Koubaa, Abdelouahid Derhab, and Mohamed Amine Ferrag. Petroblock: a blockchain-based payment mechanism for fueling smart vehicles. Applied Sciences, 11(7):3055, 2021.

[456] Jianrong Wang, Xinlei Feng, Tianyi Xu, Huansheng Ning, and Tie Qiu. Blockchain-based model for nondeterministic crowdsensing strategy with vehicular team cooperation. IEEE Internet of Things Journal, 7(9):8090–8098, 2020.

[457] Zuobin Ying, Longyang Yi, and Maode Ma. Beht: Blockchain-based efficient highway toll paradigm for opportunistic autonomous vehicle platoon. Wireless Communications and Mobile Computing, 2020, 2020.

[458] Jianxiong Guo, Xingjian Ding, and Weili Wu. Reliable traffic monitoring mechanisms based on blockchain in vehicular networks. IEEE Transactions on Reliability, 2021.

[459] Mehmet Baygin, Orhan Yaman, Nursena Baygin, and Mehmet Karakose. A blockchain-based approach to smart cargo transportation using uhf rfid. Expert Systems with Applications, 188:116030, 2022.

[460] Xi Lin, Jun Wu, Shahid Mumtaz, Sahil Garg, Jianhua Li, and Mohsen Guizani. Blockchain-based on-demand computing resource trading in iov-assisted smart city. IEEE Transactions on Emerging Topics in Computing, 2020.

[461] Q. Kong, R. Lu, F. Yin, and S. Cui. Blockchain-based privacy-preserving driver monitoring for maas in the vehicular iot. 70(4):3788–3799, 2021.

[462] Lun Li, Xiaolin Chang, Jingxian Liu, Jiqiang Liu, and Zhu Han. Bit2cv: A novel bitcoin anti-fraud deposit scheme for connected vehicles. IEEE Transactions on Intelligent Transportation Systems, 2020.

[463] Y. Fang, Y. Zhao, Y. Yu, H. Zhu, X. Du, and M. Guizani. Blockchain-based privacy-preserving valet parking for self-driving vehicles. 32(4), 2021.

[464] Rateb Jabbar, Noora Fetais, Mohamed Kharbeche, Moez Krichen, Kamel Barkaoui, and Mohammed Shinoy. Blockchain for the internet of vehicles: How to use blockchain to secure vehicle-to-everything (v2x) communication and payment? IEEE Sensors Journal, 2021.

[465] Rateb Jabbar, Moez Krichen, Mohammed Shinoy, Mohamed Kharbeche, Noora Fetais, and Kamel Barkaoui. A model-based and resource-aware testing framework for parking system payment using blockchain. In 2020 International Wireless Communications and Mobile Computing (IWCMC), pages 1252–1259. IEEE, 2020.

[466] Jelena Pajic, José Rivera, Kaiwen Zhang, and Hans-Arno Jacobsen. Eva: Fair and auditable electric vehicle charging service using blockchain. In Proceedings of the 12th ACM International Conference on Distributed and Event-based Systems, pages 262–265, 2018.

[467] Zhishang Wang, Mark Ogbodo, Huakun Huang, Chen Qiu, Masayuki Hisada, and Abderazek Ben Abdallah. Aebis: Ai-enabled blockchain-based electric vehicle integration system for power management in smart grid platform. IEEE Access, 2020.

[468] Qi Feng, Debiao He, Sherali Zeadally, and Kaitai Liang. Bpas: Blockchain-assisted privacy-preserving authentication system for vehicular ad hoc networks. IEEE Transactions on Industrial Informatics, 16(6):4146–4155, 2019.

[469] Xumin Huang, Dongdong Ye, Rong Yu, and Lei Shu. Securing parked vehicle assisted fog computing with blockchain and optimal smart contract design. IEEE/CAA Journal of Automatica Sinica, 7(2):426–441, 2020.

[470] Yuwen Pu, Tao Xiang, Chunqiang Hu, Arwa Alrawais, and Hongyang Yan. An efficient blockchain-based privacy preserving scheme for vehicular social networks. Information Sciences, 540:308–324, 2020.

[471] Yuchuan Fu, Fei Richard Yu, Changle Li, Tom H Luan, and Yao Zhang. Vehicular blockchain-based collective learning for connected and autonomous vehicles. IEEE Wireless Communications, 27(2):197–203, 2020.

[472] Jianbin Gao, Kwame Opuni-Boachie Obour Agyekum, Emmanuel Boateng Sifah, Kingsley Nketia Acheampong, Qi Xia, Xiaojiang Du, Mohsen Guizani, and Hu Xia. A blockchain-sdn-enabled internet of vehicles environment for fog computing and 5g networks. IEEE Internet of Things Journal, 7(5):4278–4291, 2019.

[473] Alessio Bonadio, Francesco Chiti, Romano Fantacci, and Vincenzo Vespri. An integrated framework for blockchain inspired fog communications and computing in internet of vehicles. Journal of Ambient Intelligence and Humanized Computing, 11(2):755–762, 2020.

[474] Rateb Jabbar, Mohamed Kharbeche, Khalifa Al-Khalifa, Moez Krichen, and Kamel Barkaoui. Blockchain for the internet of vehicles: a decentralized iot solution for vehicles communication using ethereum. Sensors, 20(14):3928, 2020.

[475] Rateb Jabbar, Moez Krichen, Mohamed Kharbeche, Noora Fetais, and Kamel Barkaoui. A model-based testing framework for validating an iot solution for blockchain-based vehicles communication. 2020.

[476] Rateb Jabbar, Moez Krichen, Mohamed Kharbeche, Noora Fetais, and Kamel Barkaoui. Un cadre de test formel pour la validation d'un système de communication inter-véhiculaire basé sur les iots et la blockchain. 2020.

[477] Rateb Jabbar, Moez Krichen, Noora Fetais, and Kamel Barkaoui. Formal verification and model-based testing techniques for validating a blockchain-based healthcare records sharing system. 2020.

[478] Rateb Jabbar, Khalifa Al-Khalifa, Mohamed Kharbeche, Wael Alhajyaseen, Mohsen Jafari, and Shan Jiang. Applied internet of things iot: Car monitoring system for modeling of road safety and traffic system in the state of qatar. In Qatar Foundation Annual Research Conference Proceedings Volume 2018 Issue 3, volume 2018, page ICTPP1072. Hamad bin Khalifa University Press (HBKU Press), 2018.

[479] Rateb Jabbar, Mohammed Shinoy, Mohamed Kharbeche, Khalifa Al-Khalifa, Moez Krichen, and Kamel Barkaoui. Urban traffic monitoring and modeling system: An iot solution for enhancing road safety. In 2019 International Conference on Internet of Things, Embedded Systems and Communications (IINTEC), pages 13–18. IEEE, 2019.

[480] Rateb Jabbar, Khalifa Al-Khalifa, Mohamed Kharbeche, Wael Alhajyaseen, Mohsen Jafari, and Shan Jiang. Real-time driver drowsiness detection for android application using deep neural networks techniques. Procedia computer science, 130:400–407, 2018.

[481] Rateb Jabbar, Mohammed Shinoy, Mohamed Kharbeche, Khalifa Al-Khalifa, Moez Krichen, and Kamel Barkaoui. Driver drowsiness detection model using convolutional neural networks techniques for android application, 2020.

[482] Kenny L. The blockchain scalability problem the race for visa-like transaction speed | by kenny l. | towards data science, 2021. [Online; Available].

[483] Sujit Biswas, Kashif Sharif, Fan Li, Boubakr Nour, and Yu Wang. A scalable blockchain framework for secure transactions in iot. IEEE Internet of Things Journal, 6(3):4650–4659, 2018.

[484] aelf - A Multi-Chain Parallel Computing Blockchain Framework. https://aelf.io/gridcn/aelf_whitepaper_EN.pdf?v=1.6, 2021. [Online; Available].

[485] Jia Kan, Shangzhe Chen, and Xin Huang. Improve blockchain performance using graph data structure and parallel mining. In 2018 1st IEEE International Conference on Hot Information-Centric Networking (HotICN), pages 173–178. IEEE, 2018.

[486] Graphchain: a framework for on-chain data management for ontochain | ontochain, 2021. [Online; Available].

[487] Nguyen Van Toan, Ung Park, and Geunwoong Ryu. Rcane: Semi-centralized network of parallel blockchain and apos. In 2018 IEEE 24th International Conference on Parallel and Distributed Systems (ICPADS), pages 1–6. IEEE, 2018.

[488] Matthias Fitzi, Peter Gazi, Aggelos Kiayias, and Alexander Russell. Parallel chains: Improving throughput and latency of blockchain protocols via parallel composition. IACR Cryptol. ePrint Arch., 2018:1119, 2018.

[489] Smart Contract Security Verification Standard . https://github.com/securing/SCSVS, 2020. [Online; Available].

[490] Xiang Fu, Huaimin Wang, Peichang Shi, and Haibo Mi. Popf: A consensus algorithm for jcledger. In 2018 IEEE Symposium on Service-Oriented System Engineering (SOSE), pages 204–209. IEEE, 2018.

[491] Naoki Shibata. Proof-of-search: combining blockchain consensus formation with solving optimization problems. IEEE Access, 7:172994–173006, 2019.

[492] AM Kudin, BA Kovalenko, and IV Shvidchenko. Blockchain technology: Issues of analysis and synthesis. Cybernetics and Systems Analysis, 55(3):488–495, 2019.

[493] Miraz Uz Zaman, Tong Shen, and Manki Min. Proof of sincerity: A new lightweight consensus approach for mobile blockchains. In 2019 16th IEEE Annual Consumer Communications & Networking Conference (CCNC), pages 1–4. IEEE, 2019.

[494] Felipe Bravo-Marquez, Steve Reeves, and Martin Ugarte. Proof-of-learning: a blockchain consensus mechanism based on machine learning competitions. In 2019 IEEE International Conference on Decentralized Applications and Infrastructures (DAPPCON), pages 119–124. IEEE, 2019.

[495] Chao Liu, Kok Keong Chai, Xiaoshuai Zhang, and Yue Chen. Proof-of-benefit: A blockchain-enabled ev charging scheme. In 2019 IEEE 89th Vehicular Technology Conference (VTC2019-Spring), pages 1–6. IEEE, 2019.

[496] Samuel Masseport, Benoît Darties, Rodolphe Giroudeau, and Jorick Lartigau. Proof of experience: empowering proof of work protocol with miner previous work. In 2020 2nd Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS), pages 57–58. IEEE, 2020.

[497] Francesco Bizzaro, Mauro Conti, and Maria Silvia Pini. Proof of evolution: leveraging blockchain mining for a cooperative execution of genetic algorithms. In 2020 IEEE International Conference on Blockchain (Blockchain), pages 450–455. IEEE, 2020.

[498] Sarwar Sayeed and Hector Marco-Gisbert. Proof of adjourn (poaj): A novel approach to mitigate blockchain attacks. Applied Sciences, 10(18):6607, 2020.

[499] Ahmed Ben Said and Abdelkarim Erradi. A probabilistic approach for maximizing travel journey wifi coverage using mobile crowdsourced services. IEEE Access, 7:82297–82307, 2019.

[500] Mohamed Abdelhedi, Rateb Jabbar, Thameur Mnif, and Chedly Abbes. Prediction of uniaxial compressive strength of carbonate rocks and cement mortar using artificial neural network and multiple linear regressions. Acta Geodynamica et Geromaterialia, 17(3):367–378, 2020.

[501] Safa Ayadi, Ahmed Ben Said, Rateb Jabbar, Chafik Aloulou, Achraf Chabbouh, and Ahmed Ben Achballah. Dairy cow rumination detection: A deep learning approach. In International Workshop on Distributed Computing for Emerging Smart Networks, pages 123–139. Springer, 2020.

[502] Emna Baccour, Fatima Haouari, Aiman Erbad, Amr Mohamed, Kashif Bilal, Mohsen Guizani, and Mounir Hamdi. An intelligent resource reservation for crowdsourced live video streaming applications in geo-distributed cloud environment. IEEE Systems Journal, 2021.

[503] Rami Hamdi, Emna Baccour, Aiman Erbad, Marwa Qaraqe, and Mounir Hamdi. Lora-rl: Deep reinforcement learning for resource management in hybrid energy lora wireless networks. IEEE Internet of Things Journal, 2021.

[504] Taotao Wang, Soung Chang Liew, and Shengli Zhang. When blockchain meets ai: Optimal mining strategy achieved by machine learning. International Journal of Intelligent Systems, 36(5):2183–2207, 2021.

[505] Zhaoyang Du, Celimuge Wu, Tsutomu Yoshinaga, Kok-Lim Alvin Yau, Yusheng Ji, and Jie Li. Federated learning for vehicular internet of things: Recent advances and open issues. IEEE Open Journal of the Computer Society, 1:45–61, 2020.

[506] Chuan Ma, Jun Li, Ming Ding, Long Shi, Taotao Wang, Zhu Han, and H Vincent Poor. When federated learning meets blockchain: A new distributed learning paradigm. arXiv preprint arXiv:2009.09338, 2020.

[507] Safa Otoum, Ismaeel Al Ridhawi, and Hussein T Mouftah. Blockchain-supported federated learning for trustworthy vehicular networks. In GLOBECOM 2020-2020 IEEE Global Communications Conference, pages 1–6. IEEE, 2020.

[508] Mouzhi Ge, Hind Bangui, and Barbora Buhnova. Big data for internet of things: a survey. Future generation computer systems, 87:601–614, 2018.

[509] Olfa Nasraoui and Chiheb-Eddine Ben N'Cir. Clustering methods for big data analytics. In Techniques, Toolboxes and Applications, page 192. Springer, 2019.

[510] Elena Karafiloski and Anastas Mishev. Blockchain solutions for big data challenges: A literature review. In IEEE EUROCON 2017-17th International Conference on Smart Technologies, pages 763–768. IEEE, 2017.

[511] Zuan Wang, Youliang Tian, and Jianming Zhu. Data sharing and tracing scheme based on blockchain. In 2018 8th international conference on logistics, Informatics and Service Sciences (LISS), pages 1–6. IEEE, 2018.

[512] Li Yue, Huang Junqin, Qin Shengzhi, and Wang Ruijin. Big data model of security sharing based on blockchain. In 2017 3rd International Conference on Big Data Computing and Communications (BIGCOM), pages 117–121. IEEE, 2017.

[513] Florent Grée, Vitaliia Laznikova, Bill Kim, Guillermo Garcia, Tom Kigezi, and Bo Gao. Cloud-based big data platform for vehicle-to-grid (v2g). World Electric Vehicle Journal, 11(2):30, 2020.

[514] Yongfeng Qian, Yingying Jiang, Long Hu, M Shamim Hossain, Mubarak Alrashoud, and Muneer Al-Hammadi. Blockchain-based privacy-aware content caching in cognitive internet of vehicles. IEEE Network, 34(2):46–51, 2020.

[515] Dongfeng Fang, Yi Qian, and Rose Qingyang Hu. Security for 5g mobile wireless networks. IEEE Access, 6:4850–4874, 2017.

[516] Dongfeng Fang and Yi Qian. 5g wireless security and privacy: Architecture and flexible mechanisms. IEEE Vehicular Technology Magazine, 15(2):58–64, 2020.

[517] Ahmed M Alwakeel, Abdulrahman K Alnaim, and Eduardo B Fernandez. A survey of network function virtualization security. In SoutheastCon 2018, pages 1–8. IEEE, 2018.

[518] Huaqun Wang, Debiao He, Jia Yu, Neal N Xiong, and Bin Wu. Rdic: A blockchain-based remote data integrity checking scheme for iot in 5g networks. Journal of Parallel and Distributed Computing, 152:1–10, 2021.

[519] Gagangeet Singh Aujla, Maninderpal Singh, Arnab Bose, Neeraj Kumar, Guangjie Han, and Rajkumar Buyya. Blocksdn: Blockchain-as-a-service for software defined networking in smart city applications. IEEE Network, 34(2):83–91, 2020.

[520] Raphael Vicente Rosa and Christian Esteve Rothenberg. Blockchain-based decentralized applications for multiple administrative domain networking. IEEE Communications Standards Magazine, 2(3):29–37, 2018.

[521] Shunliang Zhang. An overview of network slicing for 5g. IEEE Wireless Communications, 26(3):111–117, 2019.

[522] Boubakr Nour, Adlen Ksentini, Nicolas Herbaut, Pantelis A Frangoudis, and Hassine Moungla. A blockchain-based network slice broker for 5g services. IEEE Networking Letters, 1(3):99–102, 2019.

[523] Vasilios A Siris, Dimitrios Dimopoulos, Nikos Fotiou, Spyros Voulgaris, and George C Polyzos. Trusted d2d-based iot resource access using smart contracts. In 2019 IEEE 20th International Symposium on" A World of Wireless, Mobile and Multimedia Networks"(WoWMoM), pages 1–9. IEEE, 2019.

[524] Huan Cui, Zhiyong Chen, Ning Liu, and Bin Xia. Blockchain-driven contents sharing strategy for wireless cache-enabled d2d networks. In 2019 IEEE International Conference on Communications Workshops (ICC Workshops), pages 1–5. IEEE, 2019.

[525] Lixia Xie, Ying Ding, Hongyu Yang, and Xinmu Wang. Blockchain-based secure and trustworthy internet of things in sdn-enabled 5g-vanets. IEEE Access, 7:56656–56666, 2019.

[526] Vipindev Adat, Ilias Politis, Christos Tselios, Panagiotis Galiotos, and Stavros Kotsopoulos. On blockchain enhanced secure network coding for 5g deployments. In 2018 IEEE Global Communications Conference (GLOBECOM), pages 1–7. IEEE, 2018.

[527] Victor Ortega, Faiza Bouchmal, and Jose F Monserrat. Trusted 5g vehicular networks: Blockchains and content-centric networking. IEEE Vehicular Technology Magazine, 13(2):121–127, 2018.

[528] Sameerkumar Sharma, Raymond Miller, and Andrea Francini. A cloud-native approach to 5g network slicing. IEEE Communications Magazine, 55(8):120–127, 2017.