JOURNAL OF INTERNATIONAL CRISIS AND RISK COMMUNICATION RESEARCH
ISSN: 2576-0017
2024, VOL 7, NO S9

A survey: Blockchain Solutions to Secure IOV Communication

Assist. Lect. Muthana J. Khudair[1]& Associate Professor Dr. Foad Salem Mubarek[2]& Prof. Dr. Salah A. Aliesawi[3]

[1,2,3]. University of Anbar, College of Computer Science and Information Technology. mut21c1016@uoanbar.edu.iq

Abstract: The Internet of Things (IoT), smart cities, and smart transportation are just a few examples of the many possible applications for blockchain technology that go beyond cryptocurrencies and smart contracts. Blockchain can guarantee secure and autonomous car trades in the context of the Internet of Vehicles (IoV) and facilitate secure and transparent energy sharing. In addition, blockchain provides characteristics that are crucial for the creation of decentralized IoV applications and has the potential to greatly improve car energy efficiency, reduce administration costs, and guarantee resource efficiency. Despite previous studies on blockchain technology in secure IoV communication, a detailed review and latest analysis of blockchain applications in this domain are necessary. To address this gap, we present a systematic literature review of Blockchain Solutions to Secure IOV Communication, aiming to explore the current challenges in IoV and how blockchain characteristics can contribute to secure solutions. We discuss the limitations and future research directions regarding the integration of blockchain technology within IoV. To streamline our evaluation and capture the quickly expanding field of blockchain, we have included the fundamental concepts of various research articles published in the last years. Our research presents a thorough categorization of blockchain-based applications in the IoV area, which comprises privacy and security, data protection and management, vehicle management, and charging optimization. By using a structured and methodical review and content analysis of the available literature, we identify significant trends and emerging topics for future research.

Keywords: BlockChain; Internet- Of- Vehicles; systematic- literature review

1. Introduction

Vehicle network efficiency and the constraints of automated transportation systems (ITS) can be enhanced by transitioning to the Internet of Vehicles (IoVs). This new era marks a significant improvement in vehicular network capabilities . IoVs rely on two types of communication modes[1] to provide network services: communication between vehicles (V2V) and communication between vehicles and infrastructure (V2IIn either mode, vehicles collect data using on-board units (OBUs) and follow established standards such as dedicated short-range communication (DSRC) or LTE-V [2]. Up-to-the-minute information, like current traffic conditions and weather updates, can assist both vehicles and traffic controllers in making prompt decisions. These decisions may include intelligent route planning and emergency message notifications. Fig. 1 depicts communication between vehicles (V2V) and communication between vehicles and infrastructure (V2I) within the conventional Internet of Vehicles (IoV) framework, which rely on the aforementioned communication modes. Unfortunately, Despite the advantages of IoV architecture, there are still challenges associated with its applications. One such challenge pertains to the procedure of gathering data, where vehicles with malicious intent can effortlessly disseminate inaccurate information or manipulate data that is shared. As pointed out in the paper [3], this leads to various security concerns .

The use of blockchain-based technology [4], as a widely adopted distributed ledger, presents a viable solution to address the challenges faced by the Internet of Vehicles (IoVs). By providing low-cost credit support, it enhances the management of core information in the IoVs, resulting in an environment that is both see-through, unchangeable, and protects personal information [5]. For instance, all the data related to cars, such as their certificates, insurance, and other pertinent details, can be recorded on the blockchain throughout their entire lifespan [6]. Additionally, the blockchain can store data related to violations, car malfunctions, and auxiliary certificates for car dealers. Utilizing incentive mechanisms within the blockchain can enhance cooperation between vehicles, while the smart contract embedded within the blockchain ensures a secure and efficient execution process. Several studies, including [7-9], have explored the integration of blockchain technology in the Internet of Things (IoT) and related scenarios. However, some of these studies solely concentrate on how blockchain can address challenges within IoT, without explicitly highlighting its potential application in the context of the Internet of Vehicles (IoV). Conversely, other studies, such as [10-12], center more specifically on the Internet of Vehicles (IoV). For instance, [10] examines trust management in Social IoVs (SIoVs), identifying key factors for establishing trust models and presenting an overview of trending solutions. [11] introduces the intersection of IoV and blockchain, thoroughly comparing various blockchain technologies applied to IoV. Lastly, [12] offers multiple examples of blockchain applications in Vehicular Ad-hoc Networks (VANETs). In summary, past research has explored the integration of blockchain technology and Internet of Things (IoT). However, these studies fail to address the specific

Solutions to Secure of blockchain in the Internet of Vehicles (IoV). Although more recent papers have focused on blockchain to Secure in IoV, Our inquiry focuses on the query of " Secure of Blockchains in the IoVs," highlighting several aspects of how blockchain can be implemented in this context. The primary contributions of this survey are outlined as follows :

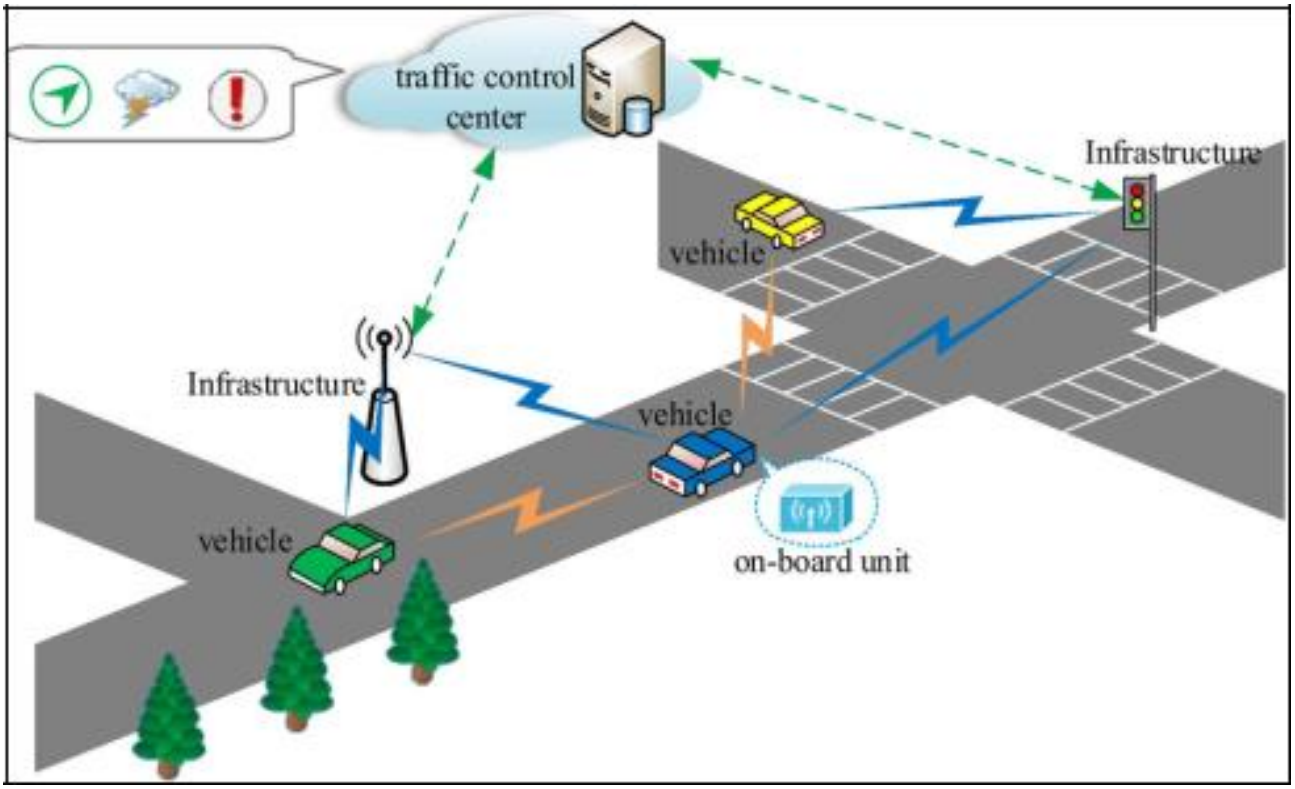

FIG. 1 A conventional layout of an automotive vehicle

1-This survey provides a succinct overview of both the Internet of Vehicles (IoV) and blockchain technology.
2-Different methods of implementing blockchain in the context of the Internet of Vehicles (IoV) are compared across various dimensions, including security and privacy.
3-Potential avenues for future research in the area of blockchain-enabled Internet of Vehicles (IoV) are identified.

This study is structured manner: Section two provides a brief introduction to Internet of Vehicles (IOV) and blockchain-based, including the design principles Related to the blockchain technology IoV architecture and features of blockchain technology. In Section three, the integration of blockchain and IoV is discussed from different perspectives, such as architecture, privacy, security, and data management. Section 4 analyzes potential future directions for blockchain implementation in IoV. Finally, Section 5 concludes this survey.

2. Background

This section presents the fundamental ideas necessary to gain a deeper comprehension of the topics discussed in this survey. The contextual knowledge centers around two key areas: the architecture and applications of the IoV, as well as the advantages and technologies of BC.

2.1. INTERNET OF VEHICLES

IoV represents a novel approach that infuses intelligence into the vehicular landscape and endeavors to surmount the principal shortcomings of Vehicular Ad Hoc Networks (VANETs) [13]: Some examples of the factors involved include scalability, interoperability, quality of service (QoS), and data processing, etc. The concept of scalability is fundamental to IoV, as it enables a wide array of applications, including but not limited to: transportation management (traffic control, parking reservation, etc.), vehicle management (personal and remote assistance), infotainment and advertising

(multimedia apps, augmented reality, etc.), road safety (cooperative collision warning, intersection coordination, etc.), and driver assistance (ADAS, parking assistance), etc.

IOV is a critical important and is based on two fundamental ideas [14]:Scalability entails the integration of novel communication methods and technologies into IoV. Through IoV, vehicles will be capable of transmitting data among themselves (Vehicle-to-Vehicle: V2V), with wireless infrastructure (Vehicle-to-Infrastructure: V2I), with base stations (Vehicle-to-Network: V2N), with pedestrians (Vehicle-to-Pedestrian: V2P), and with other devices (Vehicle-to-Device: V2D). Additionally, various cutting-edge technologies will be incorporated into vehicular communication architecture to enhance the performance of vehicular networks, including SDN, NFV, edge computing, AI, among others. Each technology will bring unique value [14]: SDN will enable programmability and flexibility, NFV will provide scalability and swifter deployment, AI will automate decision-making processes and introduce intelligent features, and edge computing will deliver high responsiveness and network off-loading.
Nevertheless, Scalability in IoV is impeded by a

lack of focus on privacy, trust, and security in current IoV architectures. Consequently, fundamental limitations with regard to trust, security, and privacy in vehicular networks persist , such as efficient authentication, trust management of vehicles, privacy preservation, and access control, among others. Furthermore, integrating various open-source technologies into vehicular communication architecture may potentially give rise to additional problems. Ultimately, enabling cooperation among vehicles to achieve efficient data transmission and resource sharing is still an unresolved issue, necessitating the development of effective incentive mechanisms [13]. Therefore, defining new mechanisms that guarantee security, privacy, trust, and cooperation in a scalable and dependable manner is paramount.

2.2. BLOCKCHAIN

As an extensively used technology, the blockchain works on a peer-to-peer network known as Bitcoin [15]. All nodes in the network possess an identical version of the blockchain data, and each one is unmodifiable. Furthermore, a public key functions as the identity of the user to ensure Protection of personal identity and confidentiality and safeguard them

privacy. Consequently, Blockchain can provide an environment that is a distributed, see-through, unchangeable, and protected system for holding information.

The block, serving as the primary unit of data in the blockchain technology, which created using the practice of secure communication through codes and algorithms, is accountable for documenting verified details about a specific financial exchange or process validated by a participant or node in the network. The structure of blocks is depicted in Fig. 2. Typically, the blockchain operates by utilizing blocks that include a block header with metadata and a block body that holds information about transactions. The block header contains multiple sets of metadata.

1- The block version number.
2- Timestamp indicating when the block was created .
3- The block's hash value.

Several have been various consensus algorithms developed suggested in the consensus process [16], including Proof of Work (PoW), Proof of Stake (PoS), Delegated Proof of Stake (DPoS), Proof of Authority (PoA), Byzantine Fault Tolerance (BFT), Practical Byzantine Fault Tolerance (PBFT), Federated Byzantine Agreement (FBA), and Directed Acyclic Graph (DAG). Table 1 outlines the typical security of different consensus mechanisms. Initially, the Bitcoin system was solely utilized for The exchange of cryptocurrencies did not include the use of smart contracts .The concept of smart contracts involves using computer programs that can automatically execute the terms of a contract when specific conditions are fulfilled. This eliminates the need for intermediaries or trusted third parties, as the execution of the contract is self-enforcing and can be programmed to follow predetermined rules and logic [17]. Contemporary platforms such as Ethereum [18] and Hyperledger [19] offer smart contract programmability, and users can deploy a diverse range of services, applications, or contracts on these platforms.

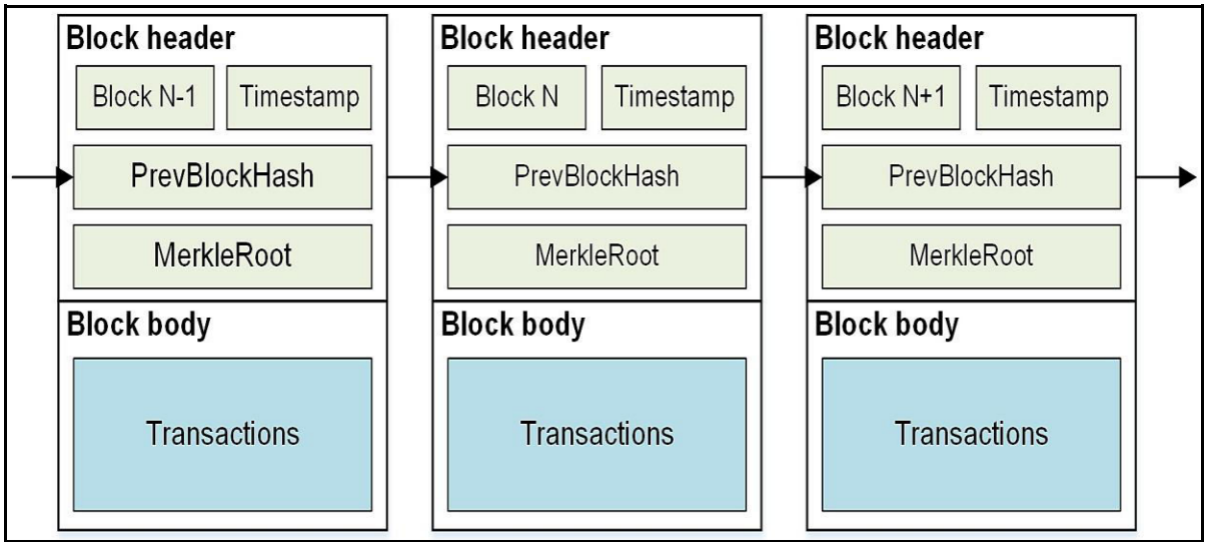

FIG. 2 Data structure of blocks

Table-1 typical security measures of different consensus mechanisms:

Consensus Mechanism	Typical Security Measures
Proof of Work (PoW)	Hash functions, computational power, decentralized network, difficulty adjustments
Proof of Stake (PoS)	Cryptographic signatures, stake-based voting, penalty systems, decentralized network
Delegated Proof of Stake (DPoS)	Stake-based voting, reputation systems, decentralized network
Proof of Authority (PoA)	Cryptographic signatures, permissioned network, trusted validators
Byzantine Fault Tolerance (BFT)	Replication, agreement protocols, threshold cryptography, decentralized network
Practical Byzantine Fault Tolerance (PBFT)	Replication, agreement protocols, threshold cryptography, decentralized network, authentication
Federated Byzantine Agreement (FBA)	Federated network, quorum slices, trust graph, digital signatures
Directed Acyclic Graph (DAG)	Transaction confirmation, asynchronous communication, reputation systems

Three types of blockchains can be distinguished based on their network access control mechanism, as outlined in [20]:

1-*Public Blockchains:* Public blockchains are open to anyone and everyone can participate in the network. There is no central authority controlling the network, and every participant has equal access to the ledger. Bitcoin and Ethereum are examples of public blockchains.

2-*Private Blockchains:* Private blockchains are controlled by a central authority or a group of entities that have permission to access the network. These types of blockchains are not open to everyone, and access to the ledger is restricted to a specific group of participants. Private blockchains are commonly used in enterprise settings to facilitate secure and efficient record-keeping and transactions.

3-*Consortium Blockchains:* Consortium blockchains are a hybrid of public and private blockchains. They are controlled by a group of entities that have permission to access the network and participate in consensus. However, unlike private blockchains, consortium blockchains allow for a larger group of participants to access the ledger. Consortium blockchains

are often used by industries or organizations that require a higher level of security and privacy than a public blockchain ca n provide, but still need to involve multiple entities in the network.

Both R3 Corda [21] and Hyperledger [19] are examples of consortium blockchains. Typically, Public blockchains are most appropriate for applications that necessitate public participation that is transparent and open. These systems involve miners who engage in the consensus process in order to receive rewards. Private blockchains, on the other hand, offer faster transaction speeds and greater information security, as the data is not visible to all. This results in safer storage and exchange of information.

The blockchain has several other classifications, including permission blockchain [22] and hybrid blockchain [23]. A permission blockchain requires nodes to obtain permission to join the system. This category includes private and consortium blockchains. As blockchain technology advances, the traditional division of blockchain architecture into public and private categories is no longer sufficient, leading to the emergence of the hybrid blockchain concept.

After analyzing IoVs, it is clear that reliable and scalable mechanisms are required to tackle security, privacy, cooperation, and trust issues. The subsequent characteristics the unique features of blockchain technology render it a distinct and remarkable innovation. appealing the technology can be employed to tackle the obstacles facing the Internet**.** Of Vehicles (IoVs) :

Decentralization: in blockchain means that all nodes in the network have equal control, removing the need for central authorities. This leads to increased transparency, security, and resistance to attacks. It also eliminates censorship and sin gle-point-of-failure risks.

Transparency: in a blockchain eliminates the need for establishing a trustworthy connection between nodes since the entire system's functioning is observable and transparent. As per the rules set within the system, nodes are unable to deceive one another.

Collective maintenance: The system is a every node that has maintenance functions participates in maintaining the system. Therefore, every individual within the system contributes to the work involved in maintaining something.

Reliable database : All network nodes possess identical copies of the blockchain ledger. Modifying the database of a single node is considered invalid, as the system automatically compares data records on each node to ensure their consistency.

Automation Smart contracts enable automation of resource and data sharing services without the need for action taken by a human being..

3.Combination the blockchain and the Internet of Values (IoVs) The following Table 2 show the analysis of the primary studies, grouped by blockchain security and IOV. The following features are highlighted: (a) authors and publication year, (b) title, (c) Categories, (d) Implemented by different

.hypothetical situations put forward in recent research studies.

Table-2 Combination the blockchain and the Internet of Values (IoVs)

(a) authors	(b) title	(c) Categories	(d) Implemented by
[31]	"BlockAPP: Using Blockchain for Authentication and Privacy Preservation in IoV"	security	BlockAPP protocol and using smart contact over Ethereum Blockchain
[32]	"Branch based blockchain technology in intelligent vehicle"		With a secure and unique crypto ID called trustworthy point f intelligent vehicles (IVTP)
[33]	"Towards a Secured Clustering Mechanism for Messages Exchange in VANET"		A secure clustering mechanism for trustworthy communicatic of messages within VANE (TCMV)
[34]	"Toward a Distributed Trust Management scheme for VANET"		A clustering mechanism that distributes trus
[35]	"Blockchain-Based Traffic Event Validation and Trust Verification for VANETs"[36]	"CreditCoin: A Privacy-	A consensus mechanism based on proof-of-event, used to validate traffic events through blockchain technology (BTEV)
		Confidenceadministration	Effect announcement network

Preserving Blockchain-Based Incentive Announcement Network for Communications of Smart Vehicles"		called Credit Coin , vehicular announcement protocol echo-announcement
[37] "Blockchain Enabled Trust-based Location Privacy Protection Scheme in VANET"		A location privacy protection scheme in VANET that utilizes blockchain to establish trust
[38] "A blockchain-based trust management with conditional privacy-preserving announcement scheme for VANETs"		anonymous cloaking region construction scheme Anonymous aggregate vehicular announcement protocol A trust management system based on blockchain that incorporates a scheme for preserving conditional privacy (BTCPS)
[39] "A Blockchain-Based Privacy-Preserving Authentication Scheme for VANETs"	Certificate administration	A scheme for authentication that preserves privacy through the use of blockchain (BPPA) all the certificate and transection are recorded permanently
[40] "An Efficient Decentralized Key Management Mechanism for VANET with Blockchain"		A mechanism for decentralized-key-managementin VANET that utilizes blockchain technology (DB-KMM)
[41] "A Privacy-preserving Trust Model based on Blockchain for VANETs"		To establish privacy preserving trust model for VANET with an anonymous reputation system that uses blockchain technology (BARS)
[42] "SCTSC: A Semi-centralized Traffic Signal Control Mode with Attribute-based Blockchain in IoVs"		A mode for traffic signal control that is semi-centralized (SCTSC) users are grouped location and direction before starting the communication
[43] "Towards Secure Blockchain-enabled Internet of Vehicles: Optimizing Consensus Management Using Reputation and Contract Theory"	Data administration	Solutions for selecting miners and verifying blocks to enhanced Delegated proof-of-stake consensus scheme (DPOS)
[44] "An Efficient Collaboration and Incentive Mechanism for Internet-of-Vehicles (IoVs) with Secured Information Exchange Based on Blockchains"		Crowdsourcing of data using mobile devices, combined with blockchain technology (MCS with blockchain) to create new model for two vehicles and a
[45] "Toward Secure Data Sharing for the IoV: A Quality-Driven Incentive Mechanism with On-Chain		novel time-window DQDA a mechanism for providing incentives suitable for low-power devices

	and Off-Chain Guarantees"		
[46]	"A Novel Debt-Credit Mechanism for Blockchain based Data-Trading in Internet of Vehicles"	Data traffic	Blockchain-based data trading and loaning system by exploiting the blockchain technology
[47]	"A Secure and Efficient Blockchain-based Data Trading Approach for Internet of Vehicles"		Achieving social welfare max by a framework for trading data that uses a consortium blockchain
[48]	"Blockchain-Based On-Demand Computing Resource Trading in IoV-Assisted Smart City"		A system for trading resources that is based on a consortium blockchain in IOV-assisted smart city be sides
[49]	"Blockchain Empowered Asynchronous Federated Learning for Secure Data Sharing in Internet of Vehicles"	Maintain privacy	A hybrid blockchain-PermiDAG a new architecture based on federated learning to relieve transmission load
[50]	"BPAS: Blockchain-Assisted Privacy-Preserving Authentication System for Vehicular Ad-Hoc Networks"	system	Blockchain-assisted privacy-preserving authentication (BPAS) to optimize verification

3-1 Blockchain and the IoVs security

The security challenges of the model of IoV that is centralized and its related components reliance trust in another party authorities can hinder the overall system availability if the authority fails. Additionally, traditional IoV models require access control mechanisms and message validation operations to maintain network security. To address these challenges, the combination of blockchain and IoV can enhance security in two ways: access control and message validation. By using blockchain, the security and privacy of connected vehicles and their related services can be improved through a decentralized, tamper-proof ledger for verifying transactions and protecting sensitive data from being compromised. Nevertheless, the integration of blockchain into the IoV also poses its own set of security challenges that need to be addressed.

With the rapid growth of the IoV, many vehicular information systems have emerged, and the level of excellence of transportation services is heavily impacted through the accessibility of the IoV. A paper [31] addresses the two primary aspects of robustness in the IoV, which are authentication and privacy preservation. The paper proposes a strong, distributed, and expandable structure that utilizes blockchain technology to achieve vehicle authentication and privacy preservation. A valid transaction is uploaded to the blockchain to confirm authorized access, and the proposed system consists of four entities: the registration server, service providers, blockchain, and vehicles. The system is comprised of three phases: registration, authentication, and authorization, which work together to maintain the system's robustness. The paper utilizes smart contracts implemented in the Remix platform to ensure security and privacy preservation during the authentication phase.

Paper [32] proposes the use of blockchain technology to address the authentication issue in communications within VANETs. The paper suggests the use of two blockchains, namely the local dynamic blockchain and the main blockchain. The local blockchain stores summary information on vehicle movement and message transmission, while unusual events are stored on the main blockchain. However, the paper identifies some challenges with this architecture. For example, the large volume of message traffic in VANETs makes it difficult to authenticate messages in real-time, and waiting times for authentication must be minimized. To address these issues, the authors propose dividing the regional dynamic blockchain into numerous concurrent blockchains, with blockchain accountable for specific geographical areas or directions of movement. Additionally, the writers propose the notion of an Intelligent Vehicle Trust Point (IVTP) for assessing the reliability of a vehicle. Nevertheless, The essay offers nothing, sufficient details on distribution of IVTPs or how to obtain them. Paper [33] proposes the use of the TCMV (trust clustering mechanism for VANET) is employed to guarantee the safety of messages in vehicular ad hoc networks by grouping trustworthy nodes together exchange by verifying the

message's accuracy of cluster heads in vehicle networks. However, solely relying on the veracity of the message may not be sufficient to determine determining whether the shared data is harmful or not.. To address this limitation, the writers of paper [34] The suggestion is to introduce a trust clustering mechanism for VANET (TCMV) that is distributed and based on blockchain technology, known as DTCMV that builds upon TCMV. The DTCMV consists of three phases: The processes of sending messages, generating blocks, and verifying blocks. In the DTCMV architecture, RSUs function as miners and have the responsibility of communicating data among each other, creating message blocks, and storing messages. The paper [35] proposes a framework called blockchain-based traffic event validation (BTEV) that leverages the benefits of blockchains. BTEV makes use of a two-pass validation method that relies on threshold-based criteria, enabling it to validate events quickly and speed up transaction processing via a two-phase consecutive transaction process. Furthermore, the framework implements a consensus mechanism called proof-of-event (PoE), which guarantees the trustworthiness of event detection. Moreover, BTEV adopts the MPT structure to improve the efficiency of confirmed event submission by RSUs to the blockchain.

3-2 Confidence administration in IoV

Traditionally, ensuring security requires relying on trusted third-party authorities. However, this approach may not always be reliable, especially during network instability or attacks. To tackle these issues, a trustless architecture has been proposed, which relies on vehicles to maintain trustworthiness of other vehicles in the network. This enables the evaluation of each vehicle's behavior. Further information on the management of trust is available in subsequent publications.

In the paper [36], the authors propose CreditCoin, an announcement network that addresses two major issues in message forwarding within IoVs. Two main challenges arise when it comes to transmitting announcements in a way that is both trustworthy and preserves user privacy. The first issue concerns finding a method to send announcements reliably while still protecting users' confidentiality. The Echo-Announcement vehicular announcement protocol provides a solution to this problem by ensuring announcements are forwarded securely and efficiently while still preserving user privacy. The second problem pertains to incentivizing vehicle nodes to forward announcements. To tackle this issue, a blockchain-based incentive mechanism has been suggested, which allows users to manage their reputation points while earning or spending coins as rewards.

The article titled [37] focuses on preventing location privacy leaks and puts forth a distributed management mechanism that combines blockchain technology and the distributed k-anonymity [1] mechanism. The authors present a trust management technique based on Dirichlet distribution that takes into account the specific characteristics of different participants. The blockchain is employed as a distributed database to store the trust values in this system. Thus, initiating and cooperating vehicles can only work with trustworthy vehicles within the anonymous cloaking region.

Paper [38] aims to address two key concerns in vehicular networks: the reliability of messages and the privacy of vehicles. To tackle the first issue, the authors propose a conditional privacy-preserving announcement protocol (BTCPS) for secure communication. The BTCPS employs message aggregation to enhance authentication and minimize network overhead, while the threshold number of vehicles improves the reliability of message announcements. Regarding the privacy concern, a blockchain-based trust management model is presented, which consists of two parts: a reputation updating algorithm and a distributed consensus algorithm. Reputation data is stored in blocks and evaluated based on direct and indirect trust values. By utilizing this method, conditional privacy, reliability, and timeliness can be achieved in vehicular networks.

3-3 Certificate administration in IoV

Every vehicle in the IoV is given an identity certificate that acts as their communication identity. Previously, certificate issuance and revocation were managed by public key infrastructure (PKI), but this method had a vulnerability in that it had a single point of failure, which compromised the network's reliability. To solve this problem, various papers have put forth solutions.

Paper [39] proposes a privacy-preserving authentication scheme called BPPA that is based on blockchain and designed for VANETs. The approach uses Chronological Merkle Tree (CMT) and Merkle Patricia Tree (MPT) to augment the blockchain structure and improve the efficiency and scalability of the system. Similarly, paper [40] proposes a decentralized key management mechanism (DB-KMM) this combines a simple authentication method with a key agreement system based on blockchain. This mechanism uses the blockchain and smart contracts to defend against Usual forms of attacks, including both internal and external attacks, tampering with public keys, denial-of-service (DoS) attacks, and collusion attacks. paper [41] proposes a reputation system that is based on blockchain and offers anonymity, and it aims to tackle three issues in VANETs: management of reputation, management of certificates, and preserving privacy between vehicle identities and certificates. This system employs three blockchains to oversee the processes of initializing, updating, revoking, and authenticating certificates. It also includes an evaluation algorithm for reputation that uses incentives to encourage active and truthful nodes, while at the same time using penalties to discourage misbehavior.

Finally, The system relies on a third-party law enforcement authority to ensure confidentiality of vehicle identities, although this approach still has some unresolved issues. Paper [42] proposes the use of a blockchain-based system for Semi-centralized Traffic Signal Control (SCTSC) that employs Ciphertext-Policy Attribute-Based Encryption (CP-ABE) to enable vehicle access control to traffic data. Users' identities are authenticated by authentication centers (AC) and trace managers (TM) before communication starts. Vehicles are grouped based on attributes; after grouping vehicles based on their attributes like position and direction, they create a temporary signal control agreement before beginning communication. Then, all users can see and confirm the decisions made by the vehicles.

3-4 Data administration in IoV

Managing data in the context of the Internet of Vehicles (IoVs) requires handling both on-chain and off-chain data. On- chai data pertains to the storage and sharing of data, while off-chain data concerns the processing and analysis of data. Nonetheless, traditional data management faces challenges in maintaining data integrity and trust when handling diverse types of vehicle data. In the context of IoVs, a paper [43] suggests a blockchain-powered data sharing platform. The paper proposes two main challenges. The first one involves identifying the appropriate miners to add blocks to the blockchain. To tackle this issue, the paper suggests a reputation-based approach to evaluate candidates based on their past interactions with other vehicles and recommended feedback from other vehicles. The reputation value of active and standby miners is higher than that of other nodes. The second challenge pertains to designing an incentive mechanism to motivate standby miners to participate in the verification process and prevent internal collusion. To address this, the paper employs contract theory to develop an incentive mechanism.

In order to address the issue of collecting vast amounts of data in situations like IoVs, mobile crowd sensing (MCS) is considered to be a potentially viable solution. Despite numerous incentive mechanisms proposed in various studies, the majority of them neglect to take into account the circumstances of an unexpected sensing task in a vehicular network. To tackle this problem, a paper [44] the study suggests a framework based on blockchain technology to facilitate effective collaboration and incentivization in the Internet of Vehicles (IoV) domain. The proposed framework includes a mechanism to motivate vehicles to participate in the general sensing task, and it securely exchanges data in the vehicular mobile crowd sensing network. The blockchain acts as both an information exchange medium between devices and the

IoT center, as well as a secure database to ensure the framework's safety. Paper [45] proposes an auction-based incentive mechanism to efficiently manage On-chain data refers to information that is stored directly on a blockchain, while off-chain data refers to data that is stored outside of the blockchain network. The mechanism focuses on maintaining data trust through the quality of the consortium blockchain. For off-chain data, the authors present an EM algorithm-based quality estimation to evaluate task data and quality.To motivate participation, the mechanism relieson the utilization of a Data Quality-Driven Auction (DQDA) model, which employs blockchain technology to maximize overall welfare while minimizing costs. To tackle security concerns related to on-chain data, a consortium blockchain is employed. A smart contract is also created to facilitate automatic data sharing and cost computation. The filtering of messages is carried out through a reverse auction process where the server takes on the role
of an auctioneer, purchasing data from users.

3-5 Data traffic in IoV

The data collected from vehicular devices can be categorized into resource and non-resource data, and it has seen a significant increase in recent years. Although the initial centralized system based on cloud technology Its purpose was to ensure the privacy of users and facilitate speedy data sharing, it requires improvements to meet current demands. Although blockchain-powered data markets for IoVs can enhance the safety of vehicular surroundings, there are still some obstacles that require attention.

In accordance with the paper [46], a supplementary debit-credit system is proposed to improve the efficacy of blockchain-driven IoV data exchange. Multi-interface stations serve as aggregators, providing swift communication and ledger storage for vehicles. Furthermore, a consortium blockchain is employed to ensure secure peer-to-peer data exchange and loan services. The pricing dilemma is tackled using a two-stage Stackelberg game model founded on a five-tier heritage structure. To address the issues highlighted in paper [47], a peer-to-peer data trading system based on a consortium blockchain is put forward. The data trading and exchange process is overseen by edge servers acting as brokers within the structure. The role of the local aggregator is to act as the authorization node responsible for gathering transaction verification information. In IoVs, vehicles can serve as carriers of resources. To address the issue of flexible allocation of computing resources, the proposal presented in paper [48] is a peer-to-peer data trading system utilizing a consortium blockchain, which enables resource sharing on an as-needed basis. To encourage user engagement, the paper introduces a two-stage Stackelberg game model to simulate the interaction between resource buyers and sellers. In the first stage, buyers establish discriminatory prices for renting resources for computing tasks. In the second stage, sellers determine the

quantity of resource transactions and transmit it to the buyer. Furthermore, the paper outlines optimal strategies for pricing and trading computing resources utilizing the Stackelberg game.

3-6 maintain utilizing blockchain for privacy in IoV

Intelligent transport systems (ITS) generate a vast amount of vehicle information, such as camera data that can improve driving experiences and record accidents. However, vehicular communication generates a contradiction between ensuring the accessibility of information and preserving its confidentiality. Therefore, the use of blockchain technology to ensure privacy preservation in IoVs is essential. By leveraging blockchain's decentralized and immutable nature, sensitive data can be secured, and data ownership can be maintained. This allows for improved trust and transparency between parties involved in the exchange and sharing of vehicle data.

In their paper [46], the authors propose PermiDAG, a hybrid blockchain system that improves data security and reduces transmission load in the vehicular environment. PermiDAG consists of two components: The proposed system utilizes a permissioned blockchain and a local directed acyclic graph (DAG) and employs the delegated proof of stake (DPoS) consensus protocol, which takes into consideration the reputation of vehicles. In order to acquire models from edge data, the authors propose an asynchronous federated learning method and employ deep reinforcement learning (DRL) to identify the node that can minimize the execution time while maximizing the accuracy of the consolidated model.. Finally, to guarantee the dependability of shared data, trained models are incorporated into the blockchain and executed via a two-step authentication process. Similarly, paper [47] proposes a new authentication framework called the blockchain-assisted privacy-preserving authentication system (BPAS). BPAS leverages the characteristics of blockchain and cryptographic primitives to implement authentication that preserves privacy, even when the trusted party is not online. BPAS ensures reliable transmission information with automatic authentication without a centralized third party.

4. Future direction

In Section 3, several security aspects of incorporating blockchain in the IoV were presented and analyzed. These integrations have the potential to improve the safety of vehicular networks. However, it is essential to emphasize future research directions in this area to further enhance the security and effectiveness of blockchain in the IoV:

Although blockchain technology has been utilized in IoVs to tackle trust and security concerns, the credibility of off-chain data in blockchain-based approaches is still unresolved. Furthermore, as the need for privacy and security in IoVs increases, the precision of off-chain data has become more critical. As an example, the authors of a recent paper (45) introduced an incentive mechanism based on DQDA that assures trust in both on-chain and off-chain data. As a result, guaranteeing the security and privacy of data on the blockchain necessitates greater attention to the security of data quality beyond the blockchain. The considerable number of transactions on each node in the blockchain-based IoV has a notable effect on energy resource consumption and data transmission or storage. Moreover, present consensus mechanisms are plagued with resource wastage, as PoW depends on physical machines to execute numerous mathematical computations to achieve the correct number. Although PoS and DPoS can decrease resource consumption, they have inadequate oversight and weak security. Lastly, the operations related to the public key can result in significant overheads. Consequently, there is a requirement for lightweight frameworks and cryptographic algorithms, as presented in references [51, 52], to be developed for blockchain-based systems.

5. Conclusion

The future of the IoV is expected to be characterized by complete connectivity of all vehicles to the internet, and blockchain technology is seen as a viable solution to support the credit system for vehicle core information at a low cost. By utilizing blockchain, the current issues with the centralized architecture of the IoV can be addressed. Although there have been previous studies on combining blockchain technology with IoVs, numerous aspects of these applications haven't been extensively investigated.

To address this gap, this study delves into This article extensively discusses and compares existing surveys on blockchain applications with a particular emphasis on their integration with the IoV, while also outlining the fundamental principles of both the IoV and blockchain. To categorize and illustrate various proposed scenarios from recent research, the study identifies six key areas, namely blockchain-based IoV security, confidence administration, certificate administration, data administration, data traffic, and privacy maintenance through blockchain in IoVs.

After conducting the survey, the study recommends a number of future research directions and open issues to address the primary challenges that the IoV may face in the coming years. This study provides a comprehensive overview of the A survey: Blockchain Solutions to Secure IOV Communication integration of blockchain technology with the IoV and highlights the potential applications of blockchain technology to enhance the security and privacy of the IoV .

References

1. J. Wang, Z. Cai, J. Yu, Achieving personalized k-anonymity-based content privacy for autonomous vehicles in cps. IEEE Trans. Ind. Inf. **16**(6), 4242–4251 (2020)

2. C. Wang, J. Li, Y. He, K. Xiao, H. Zhang, Destination prediction-based scheduling algorithms for message delivery in IoVs. IEEE Access 8, 14965–14976 (2020)

3. Z. Cai, X. Zheng, J. Yu, A diferential-private framework for urban trafc fows estimation via taxi companies. IEEE Trans. Ind. Inf. 15(12), 6492–6499 (2019)

4. S. Zhu, Z. Cai, H. Hu, Y. Li, W. Li, zkCrowd: a hybrid blockchain-based crowdsourcing platform. IEEE Trans. Ind. Inf. 16(6), 4196–4205 (2020)

5. Y. Pu, T. Xiang, C. Hu, A. Alrawais, H. Yan, An efcient blockchain-based privacy preserving scheme for vehicular social networks. Inf. Sci. 540, 308–324 (2020). https://doi.org/10.1016/j.ins.2020.05.087

A. Dorri, M. Steger, S.S. Kanhere, R. Jurdak, Blockchain: a distributed solution to automotive security and privacy. IEEE Commun. Mag. 55(12), 119–125 (2017)

6. Dorri, S.S. Kanhere, R. Jurdak, Blockchain in internet of things: challenges and Solutions (2016). arXiv:1608.05187

7. M.A. Ferrag, M. Derdour, M. Mukherjee, A. Derhab, L. Maglaras, H. Janicke, Blockchain technologies for the internet

8. of things: research issues and challenges. IEEE Internet Things J. 6(2), 2188–2204 (2019)

9. M.S. Ali, M. Vecchio, M. Pincheira, K. Dolui, F. Antonelli, M.H. Rehmani, Applications of blockchains in the internet of things: a comprehensive survey. IEEE Commun. Surv. Tutor. 21(2), 1676–1717 (2019)

10. R. Iqbal, T.A. Butt, M. Afzaal, K. Salah, Trust management in social internet of vehicles: factors, challenges, blockchain, and fog solutions. Int. J. Distrib. Sens. Netw. 15(1), 1550147719825820 (2019).

11. https://doi.org/10.1177/1550147719 825820

12. L. Mendiboure, M.A. Chalouf, F. Krief, Survey on blockchain-based applications in internet of vehicles. Comput. Electr. Eng. 84, 106646 (2020). https://doi.org/10.1016/j.compeleceng.2020.106646

13. S. Majumder, A. Mathur, A. Javaid, A study on recent applications of blockchain technology in vehicular adhoc network (VANET) (2020), pp. 293–308

14. L. Mendibourea, , M. Chaloufb , F. Kriefc, Survey on Blockchain-based Applications in Internet of Vehicles (2020),

15. pp. 3–25

16. L. Mendiboure, M. A. Chalouf, F. Krief, Towards a 5G vehicular architecture, in: 14th International Workshop, Nets4Cars/Nets4Trains/Nets4Aircraft 2019, Springer, 2019, pp. 265– 277 (2019)

17. S. Nakamoto, Bitcoin: a peer-to-peer electronic cash system. Technical report, Manubot (2019)

18. Z. Zheng, S. Xie, H. Dai, X. Chen, H. Wang, An overview of blockchain technology: architecture, consensus, and future trends, in 2017 IEEE International Congress on Big Data (BigData Congress) (IEEE, 2017), pp. 557–564

19. N. Szabo, Formalizing and securing relationships on public networks. First Monday (1997)

20. G. Wood et al., Ethereum: a secure decentralised generalised transaction ledger. Ethereum Proj. Yellow Pap.

21. 151(2014), 1–32 (2014)

22. E. Androulaki, A. Barger, V. Bortnikov, C. Cachin, K. Christidis, A. De Caro, D. Enyeart, C. Ferris, G. Laventman, Y. Manevich, et al., Hyperledger fabric: a distributed operating system for permissioned blockchains, in Proceedings of

23. the Thirteenth EuroSys Conference (2018), pp. 1–15

24. I.-C. Lin, T.-C. Liao, A survey of blockchain security issues and challenges. IJ Netw. Secur. 19(5), 653–659 (2017)

25. M. Valenta, P. Sandner, Comparison of ethereum, hyperledger fabric and corda, no. June (2017), pp. 1–8

26. H. Sukhwani, J.M. Martínez, X. Chang, K.S. Trivedi, A. Rindos, Performance modeling of PBFT consensus process for permissioned blockchain network (hyperledger fabric), in 2017 IEEE 36th Symposium on Reliable Distribute

27. H. Watanabe, S. Fujimura, A. Nakadaira, Y. Miyazaki, A. Akutsu, J. Kishigami, Blockchain contract: securing a blockchain applied to smart contracts, in 2016 IEEE International Conference on Consumer Electronics (ICCE) (2016),467–468

28. R. Sharma, S. Chakraborty, Blockapp: using blockchain for authentication and privacy preservation in IoV (2018), pp. 1–6

29. M. Singh, S. Kim, Branch based blockchain technology in intelligent vehicle. Comput. Netw. 145, 219–231 (2018). https://doi.org/10.1016/j.comnet.2018.08.016

30. R. Sharma, S. Chakraborty, Blockapp: using blockchain for authentication and privacy preservation in IoV (2018), pp. 1–6

31. M. Singh, S. Kim, Branch based blockchain technology in intelligent vehicle. Comput. Netw. 145, 219–231 (2018). https://doi.org/10.1016/j.comnet.2018.08.016

32. Kchaou, R. Abassi, S.G. El Fatmi, Towards a secured clustering mechanism for messages exchange in VANET, in 2018 32nd International Conference on Advanced Information Networking and Applications Workshops (WAINA) (2018), pp. 88–93.
33. A. Kchaou, R. Abassi, S. Guemara, Toward a distributed trust management scheme for VANET, in Proceedings of the 13th International Conference on Availability, Reliability and Security (2018), pp. 1–6
34. Y.-T. Yang, L.-D. Chou, C.-W. Tseng, F.-H. Tseng, C.-C. Liu, Blockchain-based trafc event validation and trust verifcation for vanets. IEEE Access 7, 30868–30877 (2019)
35. L. Li, J. Liu, L. Cheng, S. Qiu, W. Wang, X. Zhang, Z. Zhang, Creditcoin: a privacy-preserving blockchain-based incentive announcement network for communications of smart vehicles. IEEE Trans. Intell. Transp. Syst. 19(7), 2204–2220 (2018)
36. B. Luo, X. Li, J. Weng, J. Guo, J. Ma, Blockchain enabled trust-based location privacy protection scheme in VANET. IEEE Trans. Veh. Technol. 69(2), 2034–2048 (2020)
37. X. Liu, H. Huang, F. Xiao, Z. Ma, A blockchain-based trust management with conditional privacy-preserving announcement scheme for vanets. IEEE Internet Things J. 7(5), 4101–4112 (2020)
38. Z. Lu, Q. Wang, G. Qu, H. Zhang, Z. Liu, A blockchain-based privacy-preserving authentication scheme for VANETs. IEEE Trans. Very Large Scale Integr. (VLSI) Syst. 27(12), 2792–2801 (2019
39. Z. Ma, J. Zhang, Y. Guo, Y. Liu, X. Liu, W. He, An efcient decentralized key management mechanism for VANET with blockchain. IEEE Trans. Veh. Technol. (2020). https://doi.org/10.1109/TVT.2020.2972923
40. Z. Lu, W. Liu, Q. Wang, G. Qu, L. Zhenglin, A privacy-preserving trust model based on blockchain for vanets. IEEE Access PP, 1–1 (2018). https://doi.org/10.1109/ACCESS.2018.2864189
41. L. Cheng, J. Liu, G. Xu, Z. Zhang, W. Wang, Sctsc: a semicentralized trafc signal control mode with attribute-based blockchain in IoVs. IEEE Trans. Comput. Soc. Syst. 6(6), 1373–1385 (2019)
42. J. Kang, Z. Xiong, D. Niyato, D. Ye, D.I. Kim, J. Zhao, Toward secure blockchain-enabled internet of vehicles: optimizing consensus management using reputation and contract theory. IEEE Trans. Veh. Technol. 68(3), 2906–2920 (2019). https://doi.org/10.1109/TVT.2019.2894944
43. B. Yin, Y. Wu, T. Hu, J. Dong, Z. Jiang, An efcient collaboration and incentive mechanism for internet of vehicles (IoV) with secured information exchange based on blockchains. IEEE Internet Things J. 7(3), 1582–1593 (2020)
44. W. Chen, Y. Chen, X. Chen, Z. Zheng, Toward secure data sharing for the IoV: a quality-driven incentive mechanism with on-chain and of-chain guarantees. IEEE Internet Things J. 7(3), 1625–1640 (2019)
45. K. Liu, W. Chen, Z. Zheng, Z. Li, W. Liang, A novel debt-credit mechanism for blockchain-based data-trading in internet of vehicles. IEEE Internet Things J. 6(5), 9098–9111 (2019)
46. C. Chen, J. Wu, H. Lin, W. Chen, Z. Zheng, A secure and efcient blockchain-based data trading approach for internet of vehicles. IEEE Trans. Veh. Technol. PP, 1 (2019). https://doi.org/10.1109/TVT.2019.2927533
47. X. Lin, J. Wu, S. Mumtaz, S. Garg, J. Li, M. Guizani, Blockchain-based on-demand computing resource trading in IoVassisted smart city. IEEE Trans. Emerg. Top. Comput. 1, 1–1 (2020)
48. Y. Lu, X. Huang, K. Zhang, S. Maharjan, Y. Zhang, Blockchain empowered asynchronous federated learning for secure data sharing in internet of vehicles. IEEE Trans. Veh. Technol. 69(4), 4298–4311 (2020)
49. Q. Feng, D. He, S. Zeadally, K. Liang, Bpas: blockchain-assisted privacy-preserving authentication system for vehicular ad hoc networks. IEEE Trans. Ind. Inf. 16(6), 4146–4155 (2020)
50. Y. Liu, K. Wang, Y. Lin, W. Xu, LightChain: a lightweight blockchain system for industrial internet of things. IEEE Trans. Ind. Inf. 15(6), 3571–3581 (2019)
51. W. Yang, X. Dai, J. Xiao, H. Jin, Ldv: a lightweight DAG-based blockchain for vehicular social networks. IEEE Trans. Veh. Technol. 69(6), 5749–5759 (2020)