An Overview of Blockchain-based Applications and Architectures for VANET

Surjya Kanta Daimary
Ph.D. Scholar
Department of CSE, CIT Kokrajhar
Assam, India

Hemanta Kumar Kalita
Professor
Department of CSE, CIT Kokrajhar
Assam, India

ABSTRACT

The technology of VANET has evolved significantly, and the research is growing rapidly in present times, which helps in developing Intelligent Transport Systems and the Internet of Vehicles. The VANET helps in the effectiveness of traffic and provides better road communications, thus enhancing security, where data is being shared between moving vehicles with the help of roadside units (RSUs) and uses communication channels like WLAN and DSRC or may use cellular technologies like LTE and 5G. VANETs have several commercialization obstacles, though they can provide safety and management of traffic, as VANET cannot assure internet connectivity, and thus issues occur when using VANET-based applications used by drivers and passengers. Those applications may not guarantee a significant level of accuracy at times. Meanwhile, VANETs integrated with Blockchain has emerged as cutting-edge vehicular technology to overcome the limitations of traditional VANETs by establishing high mobility, secured connectivity among vehicles and roadside units, and providing high interactivity with personal devices. This survey provides an outline of several papers about Blockchain-based applications in VANETs further generalizes some limitations present in their work, and highlights future development in blockchain-based VANETs.

General Terms

Road Side Unit, DSRC, WLAN, LTE, 5G

Keywords

VANET, blockchain, security, Intelligent Transport System, Internet-of-Vehicles

1. INTRODUCTION

The emergence of VANETs, or Vehicular Ad-hoc Networks, aids in maintaining secure and more efficient road travel as well as facilitates the exchange of various information, such as the vehicle's speed and location, as well as various roadside unit information so that the vehicle can be aware of its surroundings and road conditions to improve communications. The VANET offers numerous benefits for in-vehicle communications, including cost and time efficiency, road safety, easier traffic management, the development of smart cities, and autonomous driving. It is recognized as the trustworthy network that automobiles use for communication on roads or in metropolitan areas. Due to their limited scalability, connectivity, intelligence, and flexibility, traditional VANETs have several technical implementation and management issues. One of the security challenges that VANETs must overcome is key management. Other security challenges include mobility, data and location verification, access control, secrecy, nonrepudiation, pseudonymity, and availability. The blockchain is a form of ledger technology that is distributed by nature, immutable, and resistant to manipulation, addressing difficulties with data security and privacy in VANETs[16]. VANET integrates blockchain to increase network security. This survey is based on the four applications of blockchain in VANET, i.e., security, privacy, trust, and incentive mechanisms, as shown in Figure 1. Recently, Blockchain has piqued the interest of corporations and the academic world because it has proficient qualities such as decentralization, immutability, resistance to temper, transparency, consensus agreement, forbearance of fault, and enhanced security.

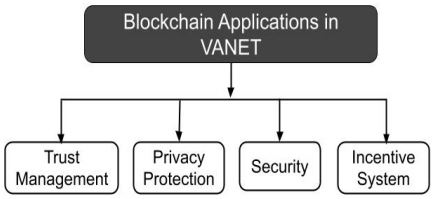

Fig. 1. Blockchain applications in VANET

This paper examines several existing blockchain-based solutions that demonstrate blockchain's potential in VANETs. Then, current research on blockchain applications in VANET concerning Trust Management, Privacy Protection, Security, and Incentive systems are discussed. Therefore, the following are the contributions of this paper:

(1) It critically analyzes and summarizes existing literature to provide current perspectives and research activities on blockchain-enabled VANET.

(2) Table 5 summarizes several previous state-of-the-art surveys to emphasize the contribution of this research.

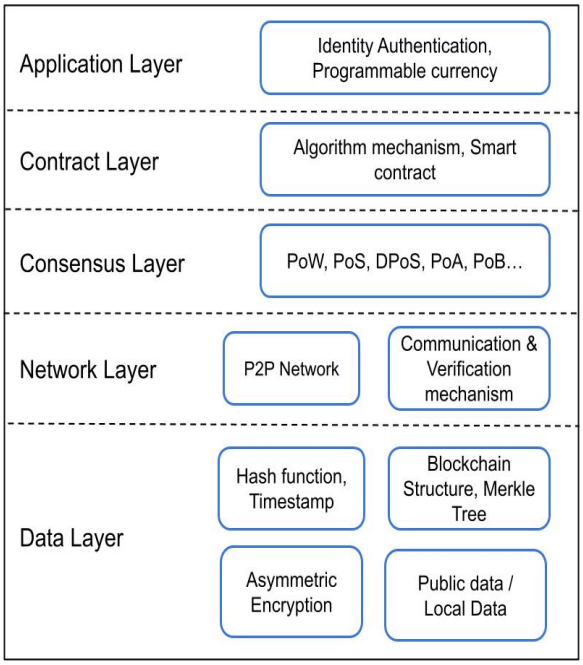

Fig. 2. Blockchain Architecture

In this paper, the second section delivers background knowledge of Vehicular Blockchain Architecture and a Blockchain structure, followed by a third section that covers a Literature Review. The discussion on challenges and future direction is included in the fourth section, and finally, the conclusion part is in the fifth section.

2. BLOCKCHAIN ARCHITECTURE

First, as depicted in Figure 2, the Vehicular Blockchain Architecture system's operation is described in the following layers: [43]
Application layer: The system's general input and output activities are made easier for end users (vehicles) through the application layer. The smart contract is started when the contract layer receives user input. The smart contract then confirms user authorization and data access restrictions.
Contract layer: This layer implements the smart contract and authenticates the stationary and moving nodes communicating with one another through the blockchain. The smart contract's logic cannot be changed after it has been performed.
Consensus layer: To build confidence among the network's nodes, the consensus method employs mathematical principles. In the Blockchain network, the block structure maintains a single copy of the ledger across all RSU-connected stationary nodes that utilize the consensus mechanism. The RSUs are dispersed organizations in charge of overseeing a region's blockchain ledgers, thereby lowering network traffic overhead. There are several blockchain consensus algorithms in use today to accomplish a variety of goals.
Network layer: Without a centralized controller, the network's nodes are all connected by hybrid P2P technology. To create linkages and exchange messages, each node utilizes a discovery protocol to locate its nearest neighbor RSU. A network layer also includes the key management and cryptography methods that are used to thwart assaults.
Data layer: This layer is responsible for keeping track of all blocks and transactions on the ledger. By utilizing the timestamp, Merkle tree structure, and hash function, the confidentiality and accuracy of the data are all assured. The system is constructed using a consortium blockchain that brings together the benefits of both the public blockchain and the private blockchain. The vehicles join the network with the help of a public key pair. In the vehicular network, this is done to assure authenticity and integrity. The stationary nodes' agreement to uphold the consistent ledger is based on a private blockchain.
Vehicle registration: By meeting the conditions, vehicles obtain the public key pair from the Certificate Authority (CA), and the CA creates the public key pair, which also registers the vehicle. When a vehicle communicates with a stationary node, Certificates are obtained with the public key pair from the vehicle and as it transmits the public key pair to a storage site across the network, the stationary node validates the public key pair it received from the certification organization.
Next, the structure of Blockchain is discussed that is depicted in Figure 3, which shows the following components of Blockchain:[17]
Block Header: Across the whole blockchain, the block header is employed to pinpoint a particular block. It controls every block on the blockchain. Miners frequently alter the nonce value used to hash a block header as part of ordinary mining activities. Following are the four main types of block information contained in the block header.
Previous Block Hash and Address: The previous block's hash links the i^{th} block to the $i + 1^{th}$ block. It simply refers to the hash of the previous (parent) block in the chain.
Timestamp: After verifying the block's contents, a timestamp is a technique that assigns a time or date of creation to digital records. A timestamp is a string of letters and numbers that specifically identifies and dates an action or a piece of text.
Nonce: Nonce is a One-time-only usage of a certain number. It is an essential part of the block's labor-proofing. It is compared to the live target if it is less than or equal to the current target. Until users find a true occurrence of a value only once, they mine, test, and eliminate it several times each second.
Merkle tree root: It is a data structure that resembles a frame made up of various data components called the Merkel Root. A Merkle Tree provides each transaction with a digital fingerprint, which collects all of the transactions into a single block. Users may use it to determine if a transaction may or cannot be included in a block. Like the hash list, the Merkle tree is a generalizable hash-based data structure, with every node-like tree structure representing a hash with the collection of data and nodes indicating the offspring of that node.
Thereafter, the following components form the core elements of blockchain:
Node: Nodes are network users that can monitor the distributed ledger and act as communication hubs during a variety of network processes. A block broadcast is issued to all network nodes whenever a miner attempts to add a new block of transactions to the blockchain.
Transaction: All agreements, contracts, and transfers of assets between parties are considered transactions. Usually, the asset is either cash or real estate. The blockchain's network duplicates the transactional data and stores it in a digital ledger.
Block: Blockchain networks' blocks resemble links in a chain. Blocks are records in the realm of cryptocurrencies that are encrypted into a hash tree and include transactions like a log book. Every day, many transactions take place in various locations

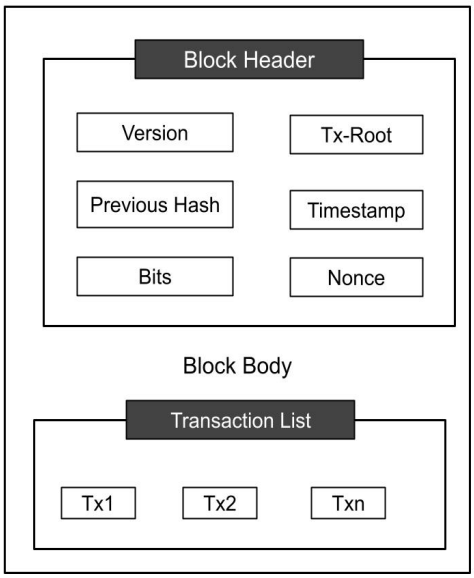

Fig. 3. Blockchain Structure

throughout the world. The block structure helps users keep track of such transactions, which is crucial for them to accomplish.
Chain: The idea of a chain defines the connections between each block in any existing blockchain structure. Additionally, the use of the hash from the previous block to connect those blocks together suggests a chaining structure.
Miners: Blockchain mining is the process of running all cryptocurrencies and verifying each stage of a transaction. The persons involved in this mining are referred to as miners. Blockchain mining is a method used to confirm each stage of a transaction while using a cryptocurrency.
Consensus: Consensus is a fault-tolerant method for achieving the required agreement between distributed processes or multi-agent systems on a single network state, like with cryptocurrency, in computer and blockchain systems. Among other things, it provides advantages for record preservation.

3. LITERATURE REVIEW

The Internet of Vehicles (IoV) is a cutting-edge paradigm that is being built as a result of the development of VANETs. Vehicles are developing into smart vehicles and ought to be capable of interconnecting with all the objects around them via a variety of access methods. Blockchain as a distributed ledger technology provides a solution to various problems that have arisen in current research. As a result, the incorporation of this technology into vehicle networks is now being researched.

3.1 Blockchain for Trust Management in VANET

As the vehicle receives the message, the trust system in vehicular networks must approve the accuracy and authenticity of the received data or information, and also the sender's credibility and dependability. Trust management is crucial for averting network attacks that might have disastrous consequences given the nature of vehicle networks. In the case of a safety-related VANET emergency warning application, for instance, the system chooses to apply the emergency brakes in the event of a near-miss or traffic hazard. The trust management system is in charge of determining how confident the emergency application should be in the information as well as the validity and reliability of the sender when it receives a warning message from other nodes. The authors[28], stated that the current trust methods utilized in VANETs are prone to several weaknesses, including trust inconsistencies between sections and false trust standards created by a collection of malicious nodes working together. To solve these issues, the authors provided ATM, a fresh local trust management strategy. ATMs use active detection and blockchain technologies. Active detection successfully filters out nearby problematic nodes and averts their dynamic participation, whereas the blockchain, in particular, guarantees that trust data is consistent across several locations. They did a numerical study to assess ATM's effectiveness. Their investigation findings demonstrate that ATMs perform more effectively than the other two trust mechanisms analyzed. It has a 90% and 95% detection accuracy for harmful activities, respectively. The authors [34], stated that the VANET's capacity to track a vehicle's precise location may be compromised if users take advantage of the convenience that Location-Based Applications (LBS) offer. They provided a trust-based, blockchain-based technique for VANET location privacy security to address this problem. They presented the Dirichlet distribution-based trust management approach by carefully evaluating the many requirements of the request and collaboration vehicles during the creation of the anonymous cloaking zone, as well as the blending of the characteristics of these two positions. Their future work is to build a secure and reliable distributed database that stores trusted data on publicly available blocks. The authors [48], used Local Dynamic Blockchain with crypto ID and IVTP, (Intelligent Vehicle Trust Point). A concept that is similar to Bitcoin is also proposed for intelligent automobiles to judge the trustworthiness of another vehicle. According to the authors, branching has the problem of storing many duplicate state changes in blocks. Using blockchain technology, the authors[49], developed a decentralized approach where CA/TA (Certificate Authority/Trusted Authority) deployed the smart contract for trust in IoV. Their method reduces transaction propagation delays while enhancing overall system throughput and efficiency. In their approach, misbehavior detection and local detection checks were not investigated. The authors[27], used PoD (Proof-of-Driving) for a scalable consensus mechanism. It permits an effective and reasonable assertion by miners in VANET. Their studies exclude applications on a certain blockchain platform, which is Hyperledger Fabric or Ethereum. The following Table 1 summarizes some of the existing Trust models in a blockchain-based VANET.

3.2 Blockchain for Privacy protection in VANET

The privacy of cars, or the privacy of information transmitted between vehicles, should be secured, and only those who have permission should be granted access. This is because one of the main goals of VANET is to preserve privacy. The difficulty for privacy-preserving approaches is maintaining accessibility while granting permitted access to the vehicle's identification and conveyed messages. [4] The authors provided a biometrics blockchain (BBC) architecture in VANET that protects the transfer of data between cars and saves archival data in a traditional and trustworthy system. Privacy is maintained in the suggested framework by utilizing biometric data to maintain information on the true distinctiveness of the sender. OMNeT++, veins, and SUMO simulations using the urban mobility model were done. The outcomes demonstrate that their innovative methodology outperforms current methodologies. The authors [15], described the Blockchain-

Table 1. Summary of existing Trust models

Reference	Application	Technique	Consensus algorithm	Storage
[46] 2018	Resolve critical message dissemination issues	Public blockchain	Proof-of-Location	Vehicles
[33] 2018	Blockchain-based Anonymous Reputation System (BARS)	Public blockchain (CerBC and RevBC)	Proofs of Presence & Absence	Vehicles & RSU
[34] 2019	Constructing anonymous cloaking region, Dirichlet distribution	Consortium blockchain	PBFT	Hyperledger
[52] 2019	BTEV , Two pass Threshold-based Event Validation technique	Multilayered Blockchain	Proof-of-Event	RSU
[49] 2020	Maintain sharded blockchains of vehicles that participate in event detection	Private blockchain	Proof-of-Work	Ethereum
[54] 2020	Bayesian Inference Model, Elliptic Curve Digital Signature Algorithm (ECDSA),	Consortium blockchain	PoW & PoS	RSU
[23] 2020	Physical Unclonable Functions, Certificates for privacy	Consortium blockchain	dPoW	RSUs
[27] 2021	Honest miners selection	Service Standard Score (Sc) Filtering technique	Proof-of-Driving	Vehicles

Assisted Privacy-Preserving Authentication System (BPAS), a special system that automates authentication in VANETs while simultaneously safeguarding vehicle privacy. This strategy is versatile and powerful. The authors extensively evaluated the efficiency and security of their suggested design in their study using the Hyperledger Fabric platform. The results support their hypothesis that VANETs can benefit from a decentralized authentication scheme. The authors[22], used the Block-VN model to work out security and privacy problems. The neighbors' degrees of confidence may be utilized to request and offer the vehicles' services, which can then be used to judge their trustworthiness. The biggest issue is the vehicles' privacy. The roadside units are informed of the ratings' performance while they are being stored. The authors[19], used a private blockchain for authentication and a public blockchain for managing event message storage. The proposed mechanism offers reduced computation and communication overheads than previous systems. Authors will duplicate their suggested work using real-time traffic statistics in the context of a vehicle, as well as study new network performance measures. A novel blockchain-based decentralized pseudonym management system was created by the authors[18]. Their system reduces the computational complexity of vehicle OBUs by shifting authentication responsibilities to RSUs. The suggested authentication approach should be combined with an efficient misbehavior detection model that can accurately identify and notify suspicious vehicles. The authors [3], used the Ethereum blockchain, ECDSA, and RSA-1024. Authentication takes only 3.1 milliseconds, while many of the previously mentioned techniques need at least 10 milliseconds. It is possible to increase the system's scalability by employing a multilevel blockchain. A few of the existing Privacy-preserving schemes are analyzed in Table 2.

3.3 Blockchain for Security in VANET

A conventional approach to vehicle network security is substantially included in the centralized server design. In a similar way to how ID-based systems need a key generation server, solutions based on public key infrastructure (PKI) require a centralized authority for verification of certificate [8]. It is inappropriate for an IoV network to employ the former since it necessitates extensive certificate administration. The latter, however, can experience serious escrow issues. The two approaches can be used to potentially lessen the severity of the issue, but it might be challenging to scale up hybrid solutions in practice. In order to address this issue, blockchain has been suggested. The authors[2], presented authentication for the Internet of Vehicles (IoV) via a secure and private blockchain-based mechanism. Cooperating with unknown or unauthorized vehicles, however, increases the risk of data theft, privacy breaches, being the target of many security assaults, etc. The proposed cooperative protocol successfully boosts system throughput while lowering PDR and latency, as evidenced by numerical evaluations, which serve as Proof-of-Concept for the technique. The authors[20], investigated the communication, consensus-building, and node authentication security concerns related to IoVs aimed at smart transportation. The Byzantine consensus approach, which is based on the time sequence and gossip protocol, is used in the development of blockchain-based IoVs to carry out consensus authentication and information transfer. This guarantees communication privacy and enhances the algorithm's and the nodes' ability to handle failures. The experimental findings demonstrated that their technique outperforms the traditional authentication process in terms of data security and IoV consensus efficacy. The results of the study offered a model response to the authentication issues in the IoVs designed for intelligent transport. The authors[36], presented a method for securing the Internet of Things (IoT) communications using the High-Performance Blockchain Consensus (HPBC). In this research, the authors gave an example of how a blockchain model may be included in the IoV communications network using a communication model for VANETs that was previously published and that employs a trustworthy routing approach to transfer packets between vehicles. They provided illustrations of the steps that they used to install HPBC on IoV nodes. The performance of the suggested model was assessed, and its impacts on the IoV network were meticulously simulated by them. The results of the simulation demonstrated that the HPBC technique worked well when used in an IoV environment. The authors[45], suggested SEA, a Secure and Efficient Authentication scheme for IoV based on blockchain. The mutual authentication between vehicles, edge nodes, and cloud servers is accomplished through SEA. Particularly when vehicles are initially authorized, the cloud server gets involved. Further, edge nodes carry out vehicle authentication by checking the authentication result in the blockchain that was recorded by the cloud, which significantly reduces the overhead of cryptographic computation and eliminates network connection delays. Moreover, session keys are negotiated between any two participating entities, protecting critical vehicle data. To demonstrate the security and effectiveness of SEA, extensive tests have been carried out. The authors[47], used the public blockchain for Mes-

Table 2. Summary of existing Privacy-preserving schemes

Reference	Application	Technique	Consensus algorithm	Storage
[44] 2018	BlockAPP & Seamless Access Control.	Ethereum blockchain	BC-based authentication Sessions pseudonyms	RSUs Cloud
[31] 2018	FICA,privacy & carpooling	Private blockchain	Vehicular Fog Computing	RSUs & cloud server
[53] 2019	Blockchain-assisted Lightweight Anonymous authentication (BLA)	Consortium blockchain	PBFT	RSUs Cloud
[15] 2019	Blockchain-assisted Privacy-preserving Authentication System (BPAS)	Consortium blockchain	PBFT	Hyperledger Fabric
[4] 2021	Biometrics Blockchain (BBC) framework	Public-private key pair	Modified Discrete Transformation (MDCT)	RSU
[2] 2021	Global Authentication Center (GAC), Local Authentication Center (LAC)	RSA-1024 digital signature, Public-private key pair	Proof-of-Concept	Vehicles

sage dissemination. Their scheme can handle the substantial transmission of event messages in real-time with a diminutive delay in VANET. Their main aim for future work is to manage the dependability of event messages using blockchain. The authors[10], used the PBFT consensus mechanism to withstand malicious tampering and data leakage. Smart contracts helped to manage the triggering environments at previously designated nodes at the time of carrying and storing data. Authors are going to strengthen the security, authentication, and message authentication processes in real-time at the time of exchanging data. The authors[29], used CP-ABE, Blockchain, and Ciphertext-based Attribute Encryption. In their approach, FADB, and IPFS can successfully eradicate the main points of failure as compared to typical cloud storage systems. The authors aim to improve the recovery function of VANET data on the blockchain and integrate the user-characteristic withdrawal function into the HECP-ABE system. Table 3 summarizes several existing Security mechanisms on VANET.

3.4 Blockchain for Incentive system in VANET

In VANET, the blockchain has applications for incentive systems besides privacy and security. Vehicles may get compensation for carrying out certain tasks; using the blockchain as an incentive mechanism, people can use it to report traffic accidents, take longer routes, or decide on an electric charging station that is less congested. The authors[37], used a Blockchain-based Emissions Allowance Trading System (B-ETS) for the trading of allowances among vehicles. Their system provides a framework for policymakers, automakers, and the EU-ETS to more effectively and safely implement carbon emission limitations. The authors aim to overcome the restrictions of this endeavor by diversifying the network's vehicles, including buses, vans, and trucks in addition to passenger cars. The authors[26], suggested a method that makes use of an Interplanetary File System's advantages (IPFS). RSUs utilize the blockchain because automobiles have a finite number of resources and take in vehicle-aggregated packets. The packets provide information about activities that take place near the vehicles. After packet verification, RSUs store event-related data in IPFS and the sender vehicle's reputation value on the blockchain. The accuracy with which a vehicle signs or initiates an event determines its reputational worth. Also, a system of rewards is advised to give money to the vehicles that respond to information concerning events. After confirming the signatures of the replies, the initiators disburse the incentives.
It could be challenging to give trustworthy announcements without disclosing users' identities. Users are frequently not very motivated to forward announcements. As a solution to these two issues, the authors [30] suggested CreditCoin, a novel reward announcement network based on blockchain with privacy-preserving characteristics. CreditCoin makes use of an effective algorithm for aggregating anonymous vehicle announcements. On the other hand, it allows non-deterministic users to sign and send messages in circumstances where confidence is only marginally established. Furthermore, it uses Blockchain to compensate users for providing traffic data, and its transactions and account information are safe. The authors [38], created a trustworthy and secure Bitcoin-based incentive system for networking services that allow cooperative vehicles to operate without delays. To operate their suggested incentive structure, the authors used scripts for Bitcoin transactions. Table 4 summarizes a few existing Incentive systems.

4. CHALLENGES AND FUTURE DIRECTION

The blockchain applications' main benefit is the possibility of improving the environment of the vehicle network. However, it is crucial to emphasize the need for more research in this field. Some of the challenges are discussed as follows:
[43] The authors used cryptography as the first security layer since it is generally regarded as an appropriate security solution for many applications. However, security that relies on cryptography is still crucial and vulnerable to many threats. Therefore, in order to identify the problematic nodes, the authors want to examine reputation and trust strategies in the future. Additionally, a system for rewards will be included to incentivize trustworthy nodes to participate in the block generation process. Future studies will concentrate on various vehicle network assaults and how to deploy blockchains while quantitatively analyzing each attack under various circumstances. In their research [27], the authors stated that there was no mention of a definite blockchain platform in the implementation, such as Hyperledger Fabric or Ethereum. Restricted storage at the vehicle node is important to look after, and the vehicles cannot store many blocks due to resource limitations. The combination of mobile edge computing and Vehicular Edge Computing and Networks (VECONs) could be followed for the purpose of enabling massive data interchange and storage in smart vehicles. A spike in blockchain latency was demonstrated by [12] as a result of raising the confirmation threshold. The huge percentage of outdated blocks that are suggested by lowering the threshold has an influence on the blockchain's resilience and stability. In future development, the traffic event validation approach should be improved. Additionally, other consensus techniques could be used to examine the study with defective RSUs. The overhead of block administration, the low block transition rate, and the high energy usage of PoW consensus are just a few of the challenges that

Table 3. Summary of existing Security mechanisms

Reference	Application	Technique	Consensus algorithm	Storage
[20] 2019	Time sequence and Gossip protocol BCA-TG	Push-Pull mode of the protocol between IoV nodes	Byzantine approach	Vehicles
[9] 2019	Reduce network latency based on priority using Cache content	Hierarchical blockchain	Practical Byzantine Fault Tolerance	RSU
[40] 2019	Reduce latency using 5G in Autonomous Vehicular Networks (AVNs)	Private blockchain	Byzantine Fault Tolerance	Vehicles & RSUs
[13] 2019	Securely exchange of messages between mobile nodes	Hierarchical blockchain	Distributed Time Consensus	RSUs
[36] 2020	SDN-based routing model integrated within ROAMER	Consortium blockchain	High-Performance Blockchain Consensus	Vehicles & RSU
[10] 2020	Credit model and voting mechanism	Private blockchain	Improved Practical Byzantine Fault Tolerance	Vehicles
[29] 2020	New data sharing architecture, FADB	Two blockchains (IC and DC) inter-blockchain & distributed consensus	HECP-ABE IPFS	RSU
[47] 2020	Security of message dissemination	Public blockchain	Proof-of-Work	Vehicles
[51] 2022	Proposed Secure Data Sharing and Efficient Throughput Algorithm	Consortium blockchain	Score Group Practical Byzantine Fault Tolerance (SG-PBFT)	RSUs
[43] 2023	Secure exchange of messages	Consortium blockchain	Vehicular network Based Consensus Algorithm (VBCA)	Edge servers

Table 4. Summary of existing Incentive systems

Reference	Application	Technique	Consensus algorithm	Storage
[39] 2018	Reliable incentive system for VDTNs (Vehicular Delay Tolerant Networks)	Bitcoin public key cryptography, ECDSA	PoW	RSUs Cloud
[6] 2018	Vehicular Cloud Computing (VCC)	Bitcoin	Utility Function	Vehicles
[30] 2018	Incentive mechanism used by CreditCoin network	Echo-Announcement Protocol	Threshold Ring Signature	RSUs Cloud
[26] 2021	Address the data storage issues using Interplanetary File System (IPFS)	Ethereum platform	PoW	RSUs

blockchain-based solutions still have to overcome. In their future work [2], the authors planned to create a blockchain-based consensus mechanism in order to gather aberrant vehicle behavior from nearby automobiles for reputation management or behavioral research. Additional security features could be added, such as the ability to thwart compromised attempts and respond to unfavorable or unusual behavior. The authors [36], investigated how altering the number of blockchain nodes will affect things on HPBC performance. To determine which blockchain model is appropriate for IoV settings, they proposed to build various consensus protocols within ROAMER and assess how well it functions in comparison to HPBC. As part of future work,[14] the authors suggested conducting research to evaluate the interactions between devices based on stationary (RSU) and mobile (OBU) devices. It will be crucial in this case to take into account the nodes' pace of movement, performance, and technical capabilities. In their research,[32] the authors proposed VANETs with a Blockchain (VNB) that require a third party, the Trusted Authority (TA), that is built on a network that is partly decentralized. As the TA has not yet experienced decentralization, the proposed VNB is not totally decentralized. The TA must be applied in a decentralized manner in order to create a fully decentralized system. In their research, [25] the authors suggested that a consensus algorithm can be used to enhance the functionality of ROA-based clustering with blockchain-based data transmission, called a ROAC-B technique.
Therefore, in order to apply blockchain in different domains more effectively, researchers should take practical implementation into account. A summary of the recent surveys on blockchain-based VANET is summarized in the following Table.

5. CONCLUSION

The protection of user privacy, trust building, and security are significant concerns for vehicular networks. Blockchain is a distributed ledger technology that is very effective in resolving the problems that are experienced in vehicular networks. Though several research have previously investigated the integration of blockchain in VANET, many areas are yet to be studied. Hence, a detailed discussion and analysis are presented with a focus on security and resilience. The architecture of vehicular blockchain structures is discussed, and then the four application areas of blockchain on VANET i.e., Trust Management, privacy protection, security, and incentive system are summarized. This survey has examined the integration of blockchain with VANET in very recent years. Further, the directions of integration-related research are then discussed. As a result, the study's attempt to leverage blockchain technology is to implement blockchain in every node of VANET. This paper attempts to clarify key points and offer knowledge that will support future blockchain-based research in VANET.

6. REFERENCES

[1] Sohail Abbas, Manar Abu Talib, Afaf Ahmed, Faheem Khan, Shabir Ahmad, and Do-Hyeun Kim. Blockchain-based

Table 5. Summary of recent surveys on Blockchain-based VANET

PAPER	FEATURES	FUTURE DIRECTIONS / LIMITATIONS
Abbas et.al., [1]	Discussed the needs for security, challenges, and potential security holes and assaults in automotive networks .	Contrasted the evaluated blockchain-based IoV authentication systems, various approaches, network topologies, assessment tools and features.
	Highlighted new research paths in IoV and VANETs, along with potential security issues.	
Wang et.al.,[50]	Addressed blockchain-based cybersecurity methods in relation to automotive networks.	Blockchain technology may aid in boosting the safety of vehicle networks.
	Evaluated and compared most recent studies that addressed secure communication, authentication, trust management, and privacy preservation.	
Alladi et.al.,[5]	Classified security frameworks: application angle, security angle, and the blockchain aspect.	Security frameworks can address requirements for low latency, data storage, reasonably priced computation.
	Frameworks are categorised according to security risks , protocols for network security, techniques for user authentication, and security justifications employed.	A development road map for academics and business experts that are looking into and producing IoV and blockchain-based vehicular networks.
	Discussed the simulation tools and platforms for blockchain-based architectures.	
Arshad et.al.,[7]	Created BCDTMS for several IoT classes, such as IoMT, IoV, IIoT, and SIoT and thoroughly evaluated.	Guidelines for creating reliable Trust Management systems that are decentralized.
	Highlighted major difficulties and crucial requirements for trust management.	
Diallo et.al.,[12]	Described the taxonomy of existing automotive network and categorized it into: centralized, dispersed, and decentralised.	The main limitations are security issues, scalability restrictions, and a lack of assessment.
Jabbar et.al., [21]	Categorized relevant research into six categories: security, energy, transport application, data management, payments and communication networks.	Discussed performance limitations, scalability and security limitations and suggested possible future directions.
	Highlighted the advantages of their study, and compared it to other literature reviews.	
Javed et.al.,[24]	Discussed Federated Learning (FL), and Blockchain integration affecting security and privacy.	Future directions in privacy and security issues, Quality of Data, near real-time decisions, handling big data and Lack of Interpretability / Justification
	ML usage inside STI is hampered by computation costs, communication costs and privacy constraints.	
Chen at.al.,[11]	Categorised three privacy issues: identity, location, and privacy.	Suggested Edge computing in blockchain to improve the efficiency of data processing.
	Summarized the main issues and the directions for future research.	Taking into account the costs, reducing the hardware and software requirements is necessary.
Mendiboure et.al., [35]	Demonstrated the improvement of inter-vehicle cooperation and resource sharing using cryptocurrencies.	Green Blockchain, Blockchain platform management, Designing new services and Integration in the future ecosystem are discussed.
	Described the key Blockchain-based incentive structures.	
Ravi et.al.,[41]	Investigated the ecology of VANET based on machanical features to improve driving safety, navigation and other roadside resources.	Advised a technique for recognizing and stopping various offensive attacks in VANET.
Saad et. al.,[42]	DLT was used as a base to construct the decentralised architecture for vehicle networks.	Research on blockchain-based 5G-enabled VANETs that have high mobility, low latency, and low power consumption may be the future step.
	Protocols used by VANETs and IoT, including handshakes, hand-offs, and data transfer are covered.	The decentralised architecture being presented might be used to create contemporary travel management systems for drones and autonomous vehicles.

authentication in internet of vehicles: A survey. *Sensors*, 21(23):7927, 2021.

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

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

[4] Abdullah Alharthi, Qiang Ni, and Richard Jiang. A privacy-preservation framework based on biometrics blockchain (bbc) to prevent attacks in vanet. *Ieee Access*, 9:87299–87309, 2021.

[5] Tejasvi Alladi, Vinay Chamola, Nishad Sahu, Vishnu Venkatesh, Adit Goyal, and Mohsen Guizani. A comprehensive survey on the applications of blockchain for securing vehicular networks. *IEEE Communications Surveys & Tutorials*, 2022.

[6] Lylia Alouache, Nga Nguyen, Makhlouf Aliouat, and Rachid Chelouah. Credit based incentive approach for v2v cooperation in vehicular cloud computing. In *Internet of Vehicles. Technologies and Services Towards Smart City: 5th International Conference, IOV 2018, Paris, France, November 20–22, 2018, Proceedings 5*, pages 92–105. Springer, 2018.

[7] Qurat-ul-Ain Arshad, Faisal Azam, Wazir Zada Khan, Muhammad Khurram Khan, and Mudassar Raza. Blockchain based decentralized trust management in iot: Systems, requirements and challenges. 2022.

[8] Nyothiri Aung, Tahar Kechadi, Sahraoui Dhelim, Tao Zhu, Aymen Dia Eddine Berini, and Tahar Guerbouz. Blockchain application on the internet of vehicles (iov). *arXiv preprint arXiv:2205.03832*, 2022.

[9] 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.

[10] Junhua Chen, Xia Zhang, and Pengfei Shangguan. Improved pbft algorithm based on reputation and voting mechanism. In *Journal of Physics: Conference Series*, volume 1486, page 032023. IOP Publishing, 2020.

[11] Wendong Chen, Haiqin Wu, Xiao Chen, and Jinfu Chen. A review of research on privacy protection of internet of vehicles based on blockchain. *Journal of Sensor and Actuator Networks*, 11(4):86, 2022.

[12] El-hacen Diallo, Omar Dib, and Khaldoun Al Agha. A scalable blockchain-based scheme for traffic-related data sharing in vanets. *Blockchain: Research and Applications*, page 100087, 2022.

[13] Ali Dorri, Salil S Kanhere, Raja Jurdak, and Praveen Gauravaram. Lsb: A lightweight scalable blockchain for iot security and anonymity. *Journal of Parallel and Distributed Computing*, 134:180–197, 2019.

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

[15] 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.

[16] Mohamed Amine Ferrag and Lei Shu. The performance evaluation of blockchain-based security and privacy systems for the internet of things: A tutorial. *IEEE Internet of Things Journal*, 8(24):17236–17260, 2021.

[17] Geeksfor Geeks. Blockchainstructure.

[18] Sonia Alice George, Steffie Maria Stephen, and Arunita Jaekel. Blockchain-based pseudonym management scheme for vehicular communication. *Electronics*, 10(13):1584, 2021.

[19] Bachira Guehguih and Hongwei Lu. Blockchain-based privacy-preserving authentication and message dissemination scheme for vanet. In *Proceedings of the 2019 5th International Conference on Systems, Control and Communications*, pages 16–21, 2019.

[20] 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.

[21] Rateb Jabbar, Eya Dhib, Ahmed Ben Said, Moez Krichen, Noora Fetais, Esmat Zaidan, and Kamel Barkaoui. Blockchain technology for intelligent transportation systems: A systematic literature review. *IEEE Access*, 10:20995–21031, 2022.

[22] Jannat Jamshaid and Nadeem Javaid. A distributed blockchain based decentralized trust management vehicular network in smart city. 2019.

[23] Uzair Javaid, Muhammad Naveed Aman, and Biplab Sikdar. A scalable protocol for driving trust management in internet of vehicles with blockchain. *IEEE Internet of Things Journal*, 7(12):11815–11829, 2020.

[24] Abdul Rehman Javed, Muhammad Abul Hassan, Faisal Shahzad, Waqas Ahmed, Saurabh Singh, Thar Baker, and Thippa Reddy Gadekallu. Integration of blockchain technology and federated learning in vehicular (iot) networks: A comprehensive survey. *Sensors*, 22(12):4394, 2022.

[25] Gyanendra Prasad Joshi, Eswaran Perumal, K Shankar, Usman Tariq, Tariq Ahmad, and Atef Ibrahim. Toward blockchain-enabled privacy-preserving data transmission in cluster-based vehicular networks. *Electronics*, 9(9):1358, 2020.

[26] Adia Khalid, Muhammad Sohaib Iftikhar, Ahmad Almogren, Rabiya Khalid, Muhammad Khalil Afzal, and Nadeem Javaid. A blockchain based incentive provisioning scheme for traffic event validation and information storage in vanets. *Information Processing & Management*, 58(2):102464, 2021.

[27] 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.

[28] Fuliang Li, Zhenbei Guo, Changsheng Zhang, Weichao Li, and Yi Wang. Atm: an active-detection trust mechanism for vanets based on blockchain. *IEEE Transactions on Vehicular Technology*, 70(5):4011–4021, 2021.

[29] 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.

[30] 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.

[31] 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.

[32] Xue Jun Li, Maode Ma, and Yong Xing Yong. A blockchain-based security scheme for vehicular ad hoc networks in smart cities. In *TENCON 2021-2021 IEEE Region 10 Conference (TENCON)*, pages 266–271. IEEE, 2021.

[33] Zhaojun Lu, Qian Wang, Gang Qu, and Zhenglin Liu. Bars: A blockchain-based anonymous reputation system for trust management in vanets. 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 98–103. IEEE, 2018.

[34] Bin Luo, Xinghua Li, Jian Weng, Jingjing Guo, and Jianfeng Ma. Blockchain enabled trust-based location privacy protection scheme in vanet. *IEEE Transactions on Vehicular Technology*, 69(2):2034–2048, 2019.

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

[36] Khaleel Mershad and Bilal Said. A blockchain model for secure communications in internet of vehicles. In *2020 IEEE/ACS 17th International Conference on Computer Systems and Applications (AICCSA)*, pages 1–6. IEEE, 2020.

[37] Lam Duc Nguyen, Amari N Lewis, Israel Leyva-Mayorga, Amelia Regan, and Petar Popovski. B-ets: A trusted blockchain-based emissions trading system for vehicle-to-vehicle networks. *arXiv preprint arXiv:2102.13477*, 2021.

[38] Youngho Park, Chul Sur, Hyunwoo Kim, and Kyung-Hyune Rhee. A reliable incentive scheme using bitcoin on cooperative vehicular ad hoc networks. *IT CoNvergence PRActice (INPRA)*, 5(4):34–41, 2017.

[39] Youngho Park, Chul Sur, and Kyung-Hyune Rhee. A secure incentive scheme for vehicular delay tolerant networks using cryptocurrency. *Security and Communication Networks*, 2018, 2018.

[40] Sandi Rahmadika, Kyeongmo Lee, and Kyung-Hyune Rhee. Blockchain-enabled 5g autonomous vehicular networks. In *2019 International Conference on Sustainable Engineering and Creative Computing (ICSECC)*, pages 275–280. IEEE, 2019.

[41] Nikhil Ravi and Chavi Kapoor. Block chain techniques to detect attacks on vanet system: A survey. In *2021 2nd International Conference on Intelligent Engineering and Management (ICIEM)*, pages 160–165. IEEE, 2021.

[42] Muhammad Saad, Muhammad Khalid Khan, and Maaz Bin Ahmad. Blockchain-enabled vehicular ad hoc networks: A systematic literature review. *Sustainability*, 14(7):3919, 2022.

[43] Naseem us Sehar, Osman Khalid, Imran Ali Khan, Faisal Rehman, Muhammad AB Fayyaz, Ali R Ansari, and Raheel Nawaz. Blockchain enabled data security in vehicular networks. *Scientific Reports*, 13(1):4412, 2023.

[44] Rohit Sharma and Suchetana Chakraborty. Blockapp: Using blockchain for authentication and privacy preservation in iov. In *2018 IEEE Globecom Workshops (GC Wkshps)*, pages 1–6. IEEE, 2018.

[45] Meng Shen, Hao Lu, Fei Wang, Huisen Liu, and Liehuang Zhu. Secure and efficient blockchain-assisted authentication for edge-integrated internet-of-vehicles. *IEEE Transactions on Vehicular Technology*, 71(11):12250–12263, 2022.

[46] Rakesh Shrestha, Rojeena Bajracharya, and Seung Yeob Nam. Blockchain-based message dissemination in vanet. In *2018 IEEE 3rd International Conference on Computing, Communication and Security (ICCCS)*, pages 161–166. IEEE, 2018.

[47] 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.

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

[49] 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*, 22(6):3616–3630, 2020.

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

[51] Guangquan Xu, Hongpeng Bai, Jun Xing, Tao Luo, Neal N Xiong, Xiaochun Cheng, Shaoying Liu, and Xi Zheng. Sg-pbft: A secure and highly efficient distributed blockchain pbft consensus algorithm for intelligent internet of vehicles. *Journal of Parallel and Distributed Computing*, 164:1–11, 2022.

[52] Yao-Tsung Yang, Li-Der Chou, Chia-Wei Tseng, Fan-Hsun Tseng, and Chien-Chang Liu. Blockchain-based traffic event validation and trust verification for vanets. *IEEE Access*, 7:30868–30877, 2019.

[53] 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.

[54] Haibin Zhang, Jiajia Liu, Huanlei Zhao, Peng Wang, and Nei Kato. Blockchain-based trust management for internet of vehicles. *IEEE Transactions on Emerging Topics in Computing*, 9(3):1397–1409, 2020.