INTERNET OF VEHICLE THINGS (IOVT) SECURITY SYSTEM WITH BLOCKCHAIN INTEGRATION

PRAKASH KRISHNA SHINDE

HEAD OF COMPUTER ENGINEERING DEPARTMENT

DR D Y PATIL POLYTECHNIC KOLHAPUR

Abstract: The automotive Internet of Things (IoT) encompasses several supporting technologies that are crucial for a wide range of significant applications, such as collaborative autonomous driving and enhanced transportation systems. The conventional centralized control system is inadequate in meeting the quality of service demands for connected vehicles due to factors such as vehicle mobility, stringent application requirements, and limited communication resources. As a result, a decentralized approach is necessary in close proximity to address the needs of delay-sensitive and mission-critical applications. A decentralized system exhibits enhanced resilience against both the single point of failure issue and malicious assaults. The capacity of developing a decentralized, transparent, and tamper-resistant system has resulted in significant interest in blockchain technology. Numerous scholarly investigations have been conducted to explore the use of blockchain technology in the management of data and transactions inside automotive contexts. Nevertheless, the implementation of blockchain technology in vehicle contexts is confronted with many technological obstacles. This article begins by providing a comprehensive overview of the basic concepts behind blockchain technology and the Internet of Things (IoT) in the context of automotive applications. Subsequently, a comprehensive examination of the extant scholarly endeavors pertaining to the integration of blockchain technology within the domain of automotive Internet of Things (IoT) is undertaken. This endeavor involves a thorough analysis of the research quandaries and technological challenges encountered in this field. Subsequently, we identify some prospective areas of study that take into account the distinctive characteristics of both blockchain technology and vehicle Internet of Things (IoT).

Keywords: blockchain; vehicular networks; IoT; decentralization, Security, Privacy, Connected Vehicles.

1. Introduction

The design of an effective vehicle IoT system has been significantly challenged by the dynamic nature and resource limitations of vehicular contexts [1, 2]. The traditional cloud

computing architecture necessitates the transfer of vehicle data to the cloud, leading to a significant delay in data transmission. The issue at hand has garnered significant interest due to the emergence of mobile edge computing (MEC) technologies in vehicle networks [3]. In order to facilitate new applications such as collaborative autonomous driving and intelligent management of traffic signals, future vehicular Internet of Things (IoT) systems must address the exceptional demands for high dependability and ultra-low latency. The application requirements exhibit variation based on factors such as application kinds, temporal considerations, geographical location, and other contextual elements, which include node density, vehicle velocity, and similar factors. The intricate and ever-changing characteristics of vehicle settings contribute to the heightened difficulty of the challenge, since a system that functions flawlessly in one road situation may encounter failures in other circumstances. An intelligent solution is necessary to effectively optimize one's actions in response to dynamic changes in the environment, particularly in an online context [4].

Current solutions for Internet of Things (IoT) applications in the automotive domain primarily emphasize the individual intelligence of each vehicle, neglecting the aspect of inter-vehicle communication. For instance, every autonomous vehicle tries to optimize its actions by relying only on the data from its own sensors. However, this approach may not effectively use the information gathered by other cars, leading to delays in adjusting to environmental changes. Due to the inherent limitations in the observational range of individual vehicles, attaining a desirable result in a dynamic environment proves to be challenging. The implementation of vehicle-to-vehicle (V2V) and vehicle-to-everything (V2X) communications has been presented as a means of facilitating the flow of information across various entities inside vehicular networks. The attainment of coordination among various entities, such as automobiles, roadside units (RSUs), base stations, pedestrians, and other relevant parties, may be seen based on the aforementioned communications. Nevertheless, the establishment of effective cooperation across diverse businesses owned by various stakeholders is hindered by challenges related to privacy and management concerns.

Federated learning, commonly referred to as collaborative learning, is a decentralized learning methodology that facilitates the exchange of information across diverse vehicles while ensuring privacy preservation [5,6]. In the context of federated learning, individual vehicles, referred to as clients, engage in the training process by using their own sensor data to develop a local model. Subsequently, these trained models are sent to a central server. The central server then consolidates local models that have been uploaded by various cars and

produces a global model. Through the dissemination of the global model across all cars, each vehicle may effectively use the collective knowledge of other vehicles while upholding privacy considerations. Federated learning may not be suitable for the majority of cases in vehicular networks owing to constraints in network resources and problems over latency, which is dependent on the central server. Hence, it is essential that cooperation inside vehicular networks be characterized by a decentralized approach.

The emergence of encryption, consensus methods, game theory, distributed systems, and communication technologies has led to the introduction of a novel distributed ledger technology (DLT) known as Blockchain. This technology was first proposed by Satoshi Nakamoto in 2008 as a means of sustaining bit coin, a well-recognized Cryptocurrency [7]. According to the illustration provided in Figure 1, the advent of Blockchain technology has introduced a novel perspective on addressing the challenges inherent in existing Internet of Things (IoT) systems [8, 9]. Blockchain is a technological innovation that establishes a connection between transaction blocks and a comprehensive collection of records via the use of cryptographic techniques. This decentralized approach ensures the preservation of transaction histories. According to the definition provided in reference [10], Blockchain is characterized as a digital, decentralized, and distributed ledger that records and appends transactions in a sequential manner, aiming to establish enduring and unalterable records. The concept of Blockchain is rooted on an openly accessible ledger that offers a reliable and enduring method for overseeing transactions within a decentralized setting. This notion has sparked considerable interest among scholars, prompting them to explore the potential applications of Blockchain technology in the realm of automobile Internet of Things (IoT).

2. Literature review

The authors Pokhrel and Choi (2011) put out a proposal for using Blockchain technology in order to facilitate Federated Learning (FL) inside a decentralized vehicular setting. The distributed ledger of Blockchain is responsible for maintaining the local models and various versions of the global models. This ledger is accessible to and can be verified by every vehicle. Vehicles function as mining entities that participate in the consensus process by validating local updates received from various workers, also known as clients. Miners are provided with a payment that is contingent upon the magnitude of local models that are collected from several clients. This incentivizes clients to engage in the verification of blocks. Reference [11] utilizes Blockchain technology to provide decentralized federated learning

(FL) in automotive contexts. The impact of the rate at which blocks arrive on the operation of the system is further examined via simulation and numerical analysis.

The deployment of intelligent transportation systems was facilitated by Zhang et al. [12] by the use of a consortium Blockchain in traffic signal regulation, specifically in the context of vehicular ad hoc networks (VANETs). The authors suggested that a decentralized traffic signal control system exhibits superior resilience compared to its centralized counterpart. A credit control method was implemented in order to mitigate the dissemination of fraudulent messages by automobiles. The traffic department implements a system whereby a commendation is granted to a vehicle that demonstrates honesty and helps to the overall efficiency of the road network by exchanging information on road conditions. A punitive measure is administered to a malevolent automobile that disseminates deceptive information. Restricted Stock Units (RSUs) function as mining agents, actively contributing to the development of the Blockchain by appending new blocks. The traffic signal is regulated by distributing the blocks across the nodes in the network, with the aim of minimizing the average waiting time for cars. Nevertheless, the effectiveness of traffic signal management may be significantly affected by the time delay caused by block verification and block announcement. Regrettably, this issue was not sufficiently addressed in the study referenced as [12].

The decentralized data sharing technique for disaster rescue objectives employing UAV-assisted vehicular networks was developed by Su et al. [13]. A Blockchain was used to enable the coordination between unmanned aerial vehicles (UAVs) and ground vehicles, therefore ensuring the safe and efficient interchange of data in regions affected by disasters. The Blockchain encompasses two distinct categories of transactions. The first component is the reporting of node misbehavior in transactions. Another kind of transaction is the regular exchange of data between nodes, which encompasses both unmanned aerial vehicles (UAVs) and ground vehicles. The consensus mechanism used is the delegated proof-of-stake (DPoS) method. In the first stage, all complete nodes engage in the process of selecting delegates, and afterwards, the delegates who are chosen assume power over the consensus mechanism. In contrast to the traditional Delegated Proof of Stake (DPoS) method, Reference [13] takes into account the credit of individual nodes and the inclusion of dissident votes inside the voting process. This design enhances the system's ability to withstand attacks from malevolent nodes.

In their study, Shen et al. (2014) examined the issue of privacy in support vector machine (SVM) training within the context of vehicular social networks (VSN). They put up a solution in the form of a consortium Blockchain-based system, which aims to decentralize the training process and eliminate the need for data sharing with external entities. The system carries out the majority of its training activities at local service providers in a non-collaborative manner, and afterwards consolidates the local training outcomes using Blockchain technology. The aforementioned notion has resemblance to federated learning, but with a notable distinction. In this case, the use of a Blockchain is employed as a means to circumvent the aggregation of data at the central server [14]. The system architecture has three distinct levels, including the VSN device layer, VSN data provider, and Blockchain service platform (BSP). The Blockchain Service Provider (BSP) enables VSN data providers to retrieve all stored information on the Blockchain while ensuring robust security measures to prevent unwanted access to VSN data.

In the study conducted by Ma et al. (2015), Blockchain technology was used as a means to decentralize the process of key management in Vehicular Ad Hoc Networks (VANETs). Blockchain technology was used to provide a decentralized storage system for public keys, while smart contract technology was leveraged to automate the process of registering and managing these keys. The key management method involves the use of three distinct entities: the car service provider, the Blockchain network, and the vehicles themselves. The supplier of automobile services implements the Blockchain network and establishes the smart contract. The vehicle service provider facilitates user interaction via the implementation of vehicle identity management, transaction data management, and public key management. The Blockchain network is established by the use of Roadside Units (RSUs) which fulfill the role of miners, using the Proof of Work (PoW) consensus process. The use of Blockchain technology facilitates the acceleration of the public key update procedure via the automation of all associated stages, which are executed through a Blockchain and smart contract. The block chain's decentralized voting system is used for the purpose of identifying and detecting malicious users.

In their study, Fu et al. (2016) examined the topic of decentralization in the context of network function virtualization management and orchestration (NFV-MANO) for the Internet of Vehicles (IoV). Blockchain-based Network Function Virtualization (NFV) architecture was suggested as a means to facilitate coordination across many Management and Orchestration (MANO) systems, eliminating the need for a centralized control server. The

framework design takes into account both the throughput and latency of the Blockchain. The processing of computational operations inside the Blockchain is facilitated via the use of edge computing technology. The primary emphasis of [16] is to the decentralization of NFV services via the use of Blockchain technologies. Consequently, it does not extensively address the concerns of the mobility of cars and its potential influence on the functioning of the Blockchain inside the framework design.

In their study, Wang et al. (2017) examined the decentralized sharing of private parking spots using Blockchain technology. In order to safeguard user privacy, the implementation described in reference [17] employs anonymous credentials, hence eliminating the need for a centralized third party credential allocator. The whole block network is maintained by a multitude of fog servers, with each fog server assuming responsibility for its designated service area by gathering and disseminating parking space data. Parking slot customers use the Blockchain network as a means to remunerate parking payments. The Blockchain network is responsible for the verification of payment transactions and subsequent recording of these validated transactions into the ledger. The primary focus of [17] is on the decentralized protocols for sharing parking slots. However, the specific mechanisms for achieving agreement are not elaborated upon in depth.

Zhang et al. (2018) introduced a Blockchain-based decentralized parking system with the objective of attaining dependability and fairness in the context of smart parking. The system has five distinct entities, namely the trusted authority, parking owner, driver, RSU, and the Blockchain network. The responsible entity assumes the responsibility of producing public parameters and keys for every parking owner and motorist. In the event of an issue arising, the authoritative body has the capability to trace the origin of the problem and ascertain the actual identities of the parking owners and drivers implicated in the situation. The use of a smart contract facilitates the attainment of automation and equity. If a motorist fulfills the need of paying the parking money, it may be certain that the driver will be allocated the matching parking place. In a similar vein, an individual who owns parking spaces receives compensation for offering private parking accommodations. The Blockchain network is comprised of interconnected Blockchain nodes that engage in collaborative efforts to achieve a state of decentralized consensus. Nevertheless, the ownership and distribution of Blockchain nodes have not been thoroughly addressed.

Deng and Gao (2019) did a preliminary examination on the topic of a Blockchain-based payment system for Vehicular Ad-Hoc Networks (VANETs). The RSUs function as complete nodes in order to maintain the integrity of the Blockchain, while the cars are responsible for generating the transaction content. The methodology for verifying a block is not addressed in the study referenced as [19]. Hassija et al. (2020) emphasized the significance of developing a Blockchain system that is lightweight in order to facilitate micro transactions. They also introduced an energy trading platform specifically designed for vehicle-to-grid networks. The tangle data structure was used to hold transactions via the utilization of a directed acyclic graph. The tip selection technique was designed in order to facilitate the inclusion of fresh transactions without the need for mining. A game theory model is used for the purpose of ascertaining prices within the domain of energy trading.

In their study, Yao et al. (2019) used a permission Blockchain framework to facilitate the implementation of a decentralized identity-as-a-service model inside automotive cloud computing environments that include numerous dispersed clouds. The system has five distinct organizations, namely the trusted authority, vehicular clouds, automobiles, vehicular cloud computing service providers, and a Blockchain network. The trustworthy authority assumes the responsibility of disseminating public parameters and safeguarding the overall security of the system. It is essential that all vehicles and service providers undergo registration with the designated trustworthy authority. Vehicle clouds are responsible for the maintenance of the Blockchain ledger. The primary issue of this system is to the reliance on a trusted authority for the upkeep of the Blockchain.

3. Proposed Model

In this section, we will provide an overview of the unresolved technological challenges in the field of vehicular Internet of Things (IoT) and discuss relevant research conducted in this area. In this analysis, we undertake a comprehensive examination of the current endeavors pertaining to the use of Blockchain technology in automotive Internet of Things (IoT) contexts. We do this by systematically categorizing existing research according to the specific challenges that Blockchain technologies aim to address.

3.1. Vehicular IoT Layers

Numerous scholarly investigations have been conducted to examine the technological complexities associated with the implementation of automotive Internet of Things (IoT) systems. In this section, we provide a concise overview of the aforementioned research,

organized based on the several levels of the Internet of Things (IoT) architecture, namely, the perception layer, networking layer, and application layer.

3.1.1. Perception Layer

The primary role of the perception layer is to observe and interpret the surrounding surroundings via the use of various sensor technologies, including as the global positioning system (GPS), laser imaging detection and ranging (LiDAR), cameras, and similar devices. High-accuracy positioning methods are necessary for controlling vehicle behaviors in delay-sensitive or mission-critical applications within the vehicular Internet of Things (IoT) context. Given the limitations of traditional positioning systems, such as GPS, in delivering adequate results, many researches have been conducted to explore methods for enhancing positioning accuracy. The suggested methodology by Jo et al. aims to enhance the precision of GPS by the use of in-vehicle sensor data. Soatti et al. (year) examined the use of information exchange among cars as a means to enhance the precision of location at each individual vehicle, a concept referred to as cooperative positioning. The information that may be sent includes traffic signals as well as stationary objects, such as non-operational vehicles in the vicinity. Shieh et al. introduced a methodology that utilizes the relative locations of cars by measuring the incoming directions of wireless signals. This is achieved via the implementation of two one-dimensional signal-direction discriminators. The authors Williams and Barth examined the necessary criteria for implementing vehicle location in contexts that include vehicles.

Several scholarly researches examine the use of compressed video sensing (CVS) technologies in the field of perception. The authors, Guo et al., used a methodology based on convolutional neural networks (CNNs) in order to enhance the precision of perception via the examination of temporal correlation among video frames. The use of roadside video sensors for vehicle sensing was examined by Alasmary et al. The researchers engaged in a discourse on the correlation between the quantity of sensors and the degree of vehicular mobility.

Cooperative perception is a sophisticated approach aimed at enhancing perception accuracy via the promotion of sensor cooperation across several vehicles. In their study, Ding et al. (year) examined the use of kinematic data within the context of cooperative perception, with the aim of fulfilling the criteria of reliability and delay constraints. Huang et al. (year) introduced a probabilistic methodology for the purpose of optimizing the selection of sensor data, with the aim of minimizing the overhead associated with collaboration while

maintaining accuracy. The researchers introduced a data selection strategy called p-consistence, which aims to strike a balance between communication overhead and system dependability. The proposed approach enables sensor-equipped cars to dynamically adjust the transmission frequency of sensor data, taking into account factors such as vehicle density, sensor penetration rate, and road layout. The simulation results demonstrate that the p-consistence approach effectively minimizes communication overhead while still providing satisfactory perception outcomes.

3.1.2. Networking Layer

The primary goal of the networking layer is to provide effective data transmission across various entities within the Internet of Things (IoT) ecosystem. There are many communication technologies that may be used for vehicle Internet of Things (IoT) applications, including cellular communications, IEEE 802.11p, and mmWave. IEEE 802.11p serves as the prevailing global standard for vehicle-to-vehicle (V2V) communications. Its primary purpose is to enhance cellular connections, particularly in situations when cellular networks are inaccessible or exhibit elevated latencies. The design of networking protocols is faced with obstacles arising from factors like as vehicle movement, restricted transmission range, and varying vehicle density. This paper examines V2V multi-hop communication protocols in vehicular contexts, specifically focusing on linked situations and delay-tolerant networks (DTN).

V2X communications may be categorized into two distinct groups, namely unicast communications and broadcast communications, based on the quantity of recipients for each transfer. The research described earlier focused on unicast communications, whereas broadcast communications are used for the distribution of control messages and safety-related messages. The dependability of broadcast communications is more challenging to accomplish in comparison to unicast communications due to the inherent difficulty, if not impossibility, of efficiently conducting retransmissions of broadcast frames at the MAC layer. It is important for the broadcast protocols to consider both dependability and efficiency, since inefficient broadcasting has the potential to give rise to the broadcast storm issue.

Several scholarly works have examined the issue of resource allocation in vehicular Internet of Things (IoT) contexts. The issue of transmission scheduling in a cognitive vehicular context was examined. The significance of effectively managing a handover in V2X

communications was deliberated over. Deep reinforcement learning was used to optimize the allocation of radio resources.

3.1.3. Application Layer

The research conducted on matters pertaining to the application layer encompasses topics such as compute offloading, task relocation, and application frameworks. A proposal was put up for a notion of edge computing that is centered on autonomous cars. Wang et al. introduced a novel methodology that employs game theory principles to enhance the efficiency of the computation offloading procedure. The technological challenges associated with task migration between distinct entities were examined by Zhang et al. This examination took into account the offloading delay and resulted in the formulation of the task migration problem as a finite horizon Markov decision process. Several novel uses for vehicle Internet of Things (IoT) have been suggested. During the discussion, a platform for automobile parking that utilizes the Internet of Things (IoT) technology was examined. A proposal was put up for a data management method that is both cooperative and decentralized. The use of vehicle Internet of Things (IoT) technologies in the context of smart city applications was examined by Khattak. There is a growing number of developing applications in the field of vehicular Internet of Things (IoT).

3.2. Blockchain and Vehicular IoT

In recent years, there has been a growing fascination in Blockchain technology. Several survey papers have been conducted to examine the available research on the use of Blockchain technology in the Internet of Things (IoT) environment. Ali et al conducted a comprehensive assessment of the use of block chains in the Internet of Things (IoT), with a specific emphasis on platforms, apps, and services that are based on Blockchain technology. Dai et al. conducted a study that specifically examined the use of Blockchain technology in fifth-generation (5G) and subsequent networks for the Internet of Things (IoT). Ferrag et al conducted a comprehensive review of Blockchain protocols specifically developed for Internet of Things (IoT) networks. The study included many application areas, including the Internet of Vehicles, Internet of Energy, Internet of Cloud, and edge computing. The study conducted by Viriyasitavat et al. primarily examined the use of Blockchain technology in enhancing the security of Internet of Things (IoT) applications, with a specific emphasis on current literature in this area. Alotaibi et al. conducted a study on the current Blockchain technologies that aim to increase the security of Internet of Things (IoT) systems. A study

was undertaken by Yang et al to examine Blockchain-based frameworks in the context of Internet services.

The use of Blockchain technology facilitates the implementation of diverse and noteworthy applications, such as the management of parking spaces and the enhancement of traffic safety. This is achieved via the decentralized administration of systems (see reference 1). Nevertheless, there is currently a lack of a thorough assessment pertaining to the use of Blockchain technology inside vehicle Internet of Things (IoT) contexts. The distinct characteristics of the vehicular Internet of Things (IoT) arise from factors such as vehicle mobility, varying node density, and stringent quality of service (QoS) demands in emergency applications. Therefore, the current Blockchain solutions designed for conventional Internet of Things (IoT) settings are inadequate in meeting the specific demands of vehicle IoT. This necessitates the undertaking of a comprehensive examination of the extant literature and technological complexities pertaining to the amalgamation of Blockchain technology with automotive Internet of Things (IoT). This section provides a comprehensive review of current scholarly investigations pertaining to the utilization of Blockchain technologies for automotive Internet of Things (IoT). These researches are categorized into three distinct groups, which align with the hierarchical structure of IoT, namely the perception layer, networking layer, and application layer.

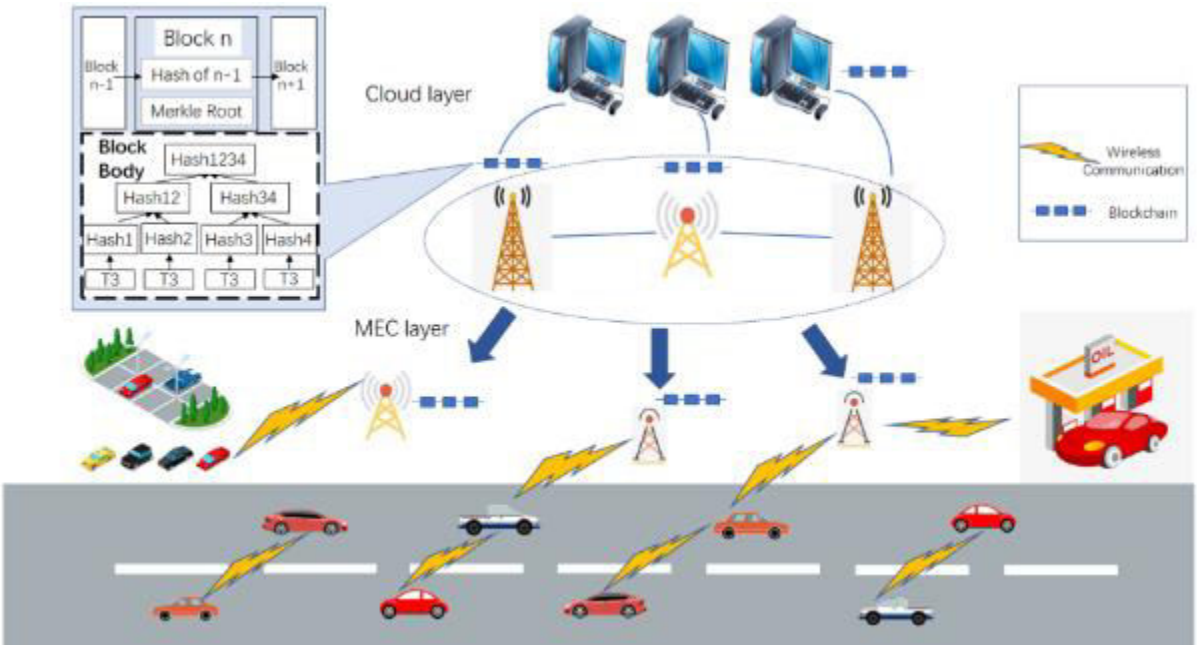

Figure 1: Blockchain in vehicular IoT.

The following factors make it difficult to perform an effective perception in a vehicle setting. To begin, a basic sensing technology is inadequate in the complicated vehicular environment, necessitating a cooperative sensing technology to attain high perception accuracy. Second, evaluating the reliability of sensor data collected from other cars has become more challenging due to the mobile nature of vehicles and the distributed nature of vehicular networks. As illustrated in 1, current Blockchain technologies are mostly concerned with resolving the issue of trust management for automobiles in distributed vehicular networks.

Table 1: Blockchain for perception layer issues in vehicular IoT

Purpose	Publication	Research Summary
Positioning	Li et al. [21]	A Blockchain-based technology to store and share the evolution of positioning errors in order to protect the security of cooperative vehicles.
Trust management	Yang et al. [22]	A Blockchain-based decentralized trust management system where RSUs work as miners to create blocks; a combination of PoS and PoW is used in achieving consensus.
	Yang et al. [23]	A traffic message validation mechanism, which is based on Blockchain that uses a PoE consensus concept.
	Liu et al. [24]	A Blockchain-based trust management scheme with the consideration of vehicle privacy.
	Xie et al. [25]	A trust management approach for real-time video report in SDN-enabled VANETs.

3.3 Networking Layer

Some research has looked at the feasibility of employing Blockchain technology to address data transmission issues in vehicle settings. Three metrics, the success chance of adding a block, the duration length of a rendezvous, and the maximum number of exchangeable blocks during a rendezvous, were considered to examine the effect of vehicle mobility on the performance of Blockchain. Most research uses block chain's primary benefits—decentralization, irreversibility, and anonymity—to boost network efficiency.

3.3.1. Decentralization Purpose

The decentralized nature of Blockchain has been used in certain research to create a system independent of a central authority. To eliminate the need for centralized servers, Li et al. created a Blockchain-based solution for data exchange in VANETs. Reference intended to develop a distributed VANET data sharing platform with improved data security and privacy and a fine-grained access control method by merging the ciphertext-based attribute encryption, Ethereum Blockchain, and the interplanetary file system (IPFS) technologies.

Security problems, according to Zhang et al., are exacerbated by the fact that VANETs are dynamic and rely on no preexisting infrastructure. They presented a block-based decentralized control plane to reach consensus among several controller nodes in complicated vehicular IoT systems, mitigating the susceptibility of the traditional centralized control plane to rogue nodes. There are three levels in this network architecture: the device layer, the area control layer, and the domain control layer. Vehicles make up the device layer, and data on those vehicles is gathered by the area control layer before being sent to the domain control layer. Multiple domain masters may reach an agreement using permission Blockchain.

3.3.2. Security Purpose

To address the potential for malicious tampering in a centralized data storage method, Zhang et al. [26] presented a consortium Blockchain-based data sharing architecture for VANETs. This is the basic structure. Every car starts by sharing information with other vehicles and RSUs in the area. The RSUs serve as designated hubs that receive data from passing cars and use it to construct new blocks. The Blockchain containing the vehicle data is produced by reaching agreement among RSUs. The RSUs employ smart contract technology to manage the information exchange. This data sharing system is based on the immutability of the Blockchain and tries to address the security concerns associated with the latter.

In order to provide private and safe data transmissions in DTNs, Rawat et al. combined Blockchain technology with named data networking. The most important part of is that block chains may be kept running without the need of RSUs or any other kind of permanent infrastructure. The vehicles are organized into many clusters, with various cluster chiefs in each. The leaders of each group are in contention to become block chain’s miners. For each cluster, one of the cluster heads is chosen to act as the miner, albeit this choice is subject to change based on the location of the vehicles. Reference is more resilient to attacks than the centralized method since all data transfers are checked by different cluster leaders.

3.4 Security or Privacy Purpose

The potential for privacy leakage for EVs during the charging process was examined by Gabay et al. [27], who presented a privacy-aware authentication problem based on Blockchain and zero-knowledge proofs. A decentralized agreement is reached with the help of Ethereum's distributed ledger, and anonymity is ensured with the help of a zero-knowledge proof-based technique. Zero-knowledge proofs provide a method through which an EV may validate its own charging behavior without disclosing its true identity. Electric vehicles, the EV service provider, and the Blockchain infrastructure are the system's constituent parts. The EV service provider first produces a secret function from the EV's data and sends it to the EV along with a proving key. The proving key is used in conjunction with the witness generated by the secret function to produce a proof by the EV. The EV communicates with a Blockchain network smart contract, which verifies the vehicle based on the evidence provided. Once the smart contract confirms the evidence, it issues a service token to the EV. Without revealing any EV details, the service token is utilized for charging.

It was suggested by Iqbal et al. [28] that VANETs use a Blockchain-based decentralized trust management mechanism to determine whether a fog vehicle is eligible for offloading activities. A scenario was explored in which RSUs delegate part of their duties to nearby fog vehicles, and an algorithm was proposed for selecting fog vehicles that takes into consideration both the workload and the reputation of vehicles. When RSUs are used as miners, a consortium Blockchain is used to keep track of vehicle credibility. Multiple RSUs may come to an agreement using a proof-of-elapsed-time (PoET) method. To determine which miner will be responsible for adding new blocks to the network, PoET assigns each miner a random waiting time. The Blockchain records both financial transactions and user feedback in separate ledgers. Information on the chosen fog vehicles, offloading requests, computing requirements, job due dates, and more are all recorded in a transaction ledger. Task offloading node selection takes into account the social reputation ratings of available cars in the reputation ledger.

In this paper, we offer a Blockchain-based remote attestation approach for trustworthy computing in automotive contexts. There are two phases to the attestation procedure. Identity authentication is the initial stage, and it ensures that a node is using a legitimate identify. In the next phase, participants will debate and add new blocks to the ledger. Each node in [28]'s Blockchain is uniquely recognized by an attestation identification key, allowing for a distributed record of access control decisions. To verify the concept, experiments are carried out using a real-world V2X setting in mind.

4. Discussions

Only a few of research articles address the topic of vehicle miners. Present research essentially presupposes that automobiles are linked to the Blockchain system by means of RSUs. Managing block chains in decentralized systems is the subject of a small number of research papers. Only one publication makes use of actual trials as part of their review process, while the rest rely on either theoretical analysis or computer simulations. Existing research does not sufficiently explore how well block generation throughput and how quickly agreement may be reached.

We provide a brief overview of the research' shortcomings.

Most research has only touched on the value of Blockchain for certain uses, avoiding the nitty-gritty of Blockchain upkeep and its effect on system performance. More research should be focused on actual Blockchain system implementations, since computer models can only disclose so many issues.

Insufficient attention is paid to how Blockchain may be implemented in a decentralized system. Distributed contexts, such as vehicle ad hoc networks, cannot make use of the miners that are often assumed to be RSUs or cloud servers in most research.

The maintenance of block chains in a wireless setting is a complex and little-studied area. Blockchain systems must broadcast the transaction records to all the miners in order to create a decentralized consensus. This calls for a substantial communication bandwidth, which is challenging to provide in a vehicle's constrained environment.

The effect of mobile access on Blockchain efficiency is not well studied. Discussion of the issue of "how to reach a consensus in a mobile environment" is warranted.

5. Conclusion

Block chain’s potential to provide a decentralized, open, and unchangeable system has piqued the curiosity of academics and businesses alike. When used to the Internet of Things (IoT), Blockchain enables a wide variety of novel features and use cases. Meanwhile, there are significant hurdles to overcome in the creation of an effective Blockchain system due to the fluid nature of vehicle situations.

Currently available literature discusses how Blockchain technology may be used to address issues at the IoT's perception, networking, and application levels. When it comes to the

perception layer, Blockchain is often employed to either increase the perception accuracy via data sharing across cars or to address the trust management problem in decentralized settings. Blockchain is mostly used to the networking layer to address decentralized networking, network security, and networking incentive problems. Many researches examine application-layer problems for the decentralization, security/privacy, and auditing objectives. The design of an effective Blockchain system aimed at a particular scenario is still an open challenge, since various applications involve different sorts of network entities and need varying degrees of QoS. Effective integration of many IoT layers into future automotive IoT systems is essential. For instance, if numerous cars need to work together to get accurate perception of a complicated environment, Blockchain technology might be used to facilitate agreement among them. Therefore, the use of Blockchain technology to vehicle Internet of Things systems still needs more study.

However, when new forms of communication and processing arise, it is crucial to consider how best to use these technologies to enable Blockchain in mobile contexts, such as cars. To meet the ultra-reliable low-latency needs of vehicular IoT applications, Blockchain protocols that take into account the specifics of a vehicle's surroundings should be developed. There has to be more research done into the problems of ensuring block chain’s functioning in the chaotic settings of a moving vehicle.

6. References

[1]. Gubbi, J.; Buyya, R.; Marusic, S.; Palaniswam, M. Internet of Things (IoT): A vision, architectural elements, and future directions. Future Gener. Comput. Syst. 2013, 29, 1645–1660.

[2]. Lee, I.; Lee, K. The Internet of Things (IoT): Applications, investments, and challenges for enterprises. Bus. Horizons 2015, 58, 431–440.

[3]. Onieva, J.A.; Rios, R.; Roman, R.; Lopez, J. Edge-Assisted Vehicular Networks Security. IEEE Internet Things J. 2019, 6, 8038–8045.

[4]. Wu, C.; Liu, Z.; Zhang, D.; Yoshinaga, T.; Ji, Y. Spatial Intelligence towards Trustworthy Vehicular IoT. IEEE Commun. Mag. 2018, 56, 22–27.

[5]. Du, Z.; Wu, C.; Yoshinaga, T.; Yau, K.-L.A.; Ji, Y.; Li, J. Federated Learning for Vehicular Internet of Things: Recent Advances and Open Issues. IEEE Open J. Comput. Soc. 2020, 1, 45–61.

[6]. McMahan, H.B.; Moore, E.; Ramage, D.; Hampson, S.; Arcas, B.A.Y. Communication-Efficient Learning of Deep Networks from Decentralized Data. In Proceedings of the 20th International Conference on Artificial Intelligence and Statistics, Ft. Lauderdale, FL, USA, 20–22 April 2017; pp. 1273–1282.

[7]. Tschorsch, F.; Scheuermann, B. Bitcoin and beyond: A technical survey on decentralized digital currencies. IEEE Commun. Surv. Tutorials 2016, 18, 2084–2123.

[8]. Khan, M.A.; Salah, K. IoT security: Review, blockchain solutions, and open challenges. Future Gener. Comput. Syst. 2018, 82, 395–411.

[9]. Wamba, S.F.; Kamdjoug, J.R.K.; Bawack, R.E.; Keogh, J.G. Bitcoin, Blockchain and Fintech: A systematic review and case studies in the supply chain. Prod. Plan. Control 2020, 31, 115–142.

[10]. Treiblmaier, H. The impact of the blockchain on the supply chain: A theory-based research framework and a call for action. Supply Chain Manag. 2018, 23, 545–559.

[11] Pokhrel, S.R.; Choi, J. Federated Learning with Blockchain for Autonomous Vehicles: Analysis and Design Challenges. IEEE Trans. Commun. 2020.

[12]. Zhang, X.; Wang, D. Adaptive Traffic Signal Control Mechanism for Intelligent Transportation Based on a Consortium Blockchain. IEEE Access 2019, 7, 97281–97295.

[13]. Su, Z.; Wang, Y.; Xu, Q.; Zhang, N. LVBS: Lightweight Vehicular Blockchain for Secure Data Sharing in Disaster Rescue. IEEE Trans. Dependable Secur. Comput. 2020.

[14]. Shen, M.; Zhang, J.; Zhu, L.; Xu, K.; Tang, X. Secure SVM Training over Vertically-Partitioned Datasets using Consortium Blockchain for Vehicular Social Networks. IEEE Trans. Veh. Technol. 2020.

[15]. Ma, Z.; Zhang, J.; Guo, Y.; Liu, Y.; Liu, X.; He, W. An Efficient Decentralized Key Management Mechanism for VANET with Blockchain. IEEE Trans. Veh. Technol. 2020.

[16]. Fu, X.; Yu, R.; Wang, J.; Qi, Q.; Liao, J. Performance Optimization for Blockchain-Enabled Distributed Network Function Virtualization Management and Orchestration (NFV-MANO). IEEE Trans. Veh. Technol. 2020.

[17]. Wang, L.; Lin, X.; Zima, E.; Ma, C. Towards Airbnb-Like Privacy-Enhanced Private Parking Spot Sharing Based on Blockchain. IEEE Trans. Veh. Technol. 2020, 69, 11–23.

[18]. Zhang, C.; Zhu, L.; Xu, C.; Zhang, C.; Sharif, K.; Wu, H.; Westermann, H. BSFP: Blockchain-Enabled Smart Parking with Fairness, Reliability and Privacy Protection. IEEE Trans. Veh. Technol. 2020.

[19]. Deng, X.; Gao, T. Electronic Payment Schemes Based on Blockchain in VANETs. IEEE Access 2020, 8, 38296–38303.

[20]. Zhang, X.; Chen, X. Data Security Sharing and Storage Based on a Consortium Blockchain in a Vehicular Ad-hoc Network. IEEE Access 2019, 7, 581–58254.

[21]. Huang, H.; Li, H.; Shao, C.; Sun, T.; Fang, W.; Dang, S. Data Redundancy Mitigation in V2X Based Collective Perceptions. IEEE Access 2020, 8, 13405–13418.

[22]. Yang, W.; Aghasian, E.; Garg, S.; Herbert, D.; Disiuta, L.; Kang, B. A Survey on Blockchain-Based Internet Service Architecture: Requirements, Challenges, Trends, and Future. IEEE Access 2019, 7, 75845–75872.

[23]. Yang, Z.; Yang, K.; Lei, L.; Zheng, K.; Leung, V.C.M. Blockchain-Based Decentralized Trust Management in Vehicular Networks. IEEE Internet Things J. 2019, 6, 1495–1505.

[24]. Liu, X.; Huang, H.; Xiao, F.; Ma, Z. A Blockchain-Based Trust Management With Conditional Privacy-Preserving Announcement Scheme for VANETs. IEEE Internet Things J. 2020, 7, 4101–4112.

[25]. Xie, L.; Ding, Y.; Yang, H.; Wang, X. Blockchain-Based Secure and Trustworthy Internet of Things in SDN-Enabled 5G-VANETs. IEEE Access 2019, 7, 56656–56666.

[26]. Hassija, V.; Saxena, V.; Chamola, V.; Yu, R. A Parking Slot Allocation Framework Based on Virtual Voting and Adaptive Pricing Algorithm. IEEE Trans. Veh. Technol. 2020.

[27]. Gabay, D.; Akkaya, K.; Cebe, M. Privacy-preserving Authentication scheme for Connected Electric Vehicles Using Blockchain and Zero Knowledge Proofs. IEEE Trans. Veh. Technol. 2020.

[28]. Xu, C.; Liu, H.; Li, P.; Wang, P. A Remote Attestation Security Model Based on Privacy-Preserving Blockchain for V2X. IEEE Access 2018, 6, 67809–67818