Security Challenges Facing Blockchain Based-IoV Network: A Systematic Review

Hamza El Mazouzi[1], Anass Khannous[2], Khalid Amechnoue[3], Anass Rghioui[4]
RMIA Team, National School of Applied Sciences, Tangier, Morocco[1, 2, 3]
SIRC Research Team, Hassania School of Public Works, Casablanca, Morocco[4]

***Abstract*—The Internet of Vehicles (IoV) is an innovative concept aimed at addressing the critical problem of traffic congestion. IoV applications are part of a connected network that collects relevant data from various smart sensors installed in connected vehicles. This information is freely and easily exchanged between vehicles, which leads to improved traffic management and a reduction in traffic accidents. As the IoV technology continues to grow, the amount of data collected will increase, presenting new challenges for data privacy and security. The use of blockchain technology has been proposed as a solution, as its decentralized and distributed architecture has been proven reliable with cryptocurrencies such as Bitcoin. However, studies have shown that blockchain alone may not be sufficient to address privacy and security concerns, and there are currently no tools available to evaluate its performance in an IoV simulation environment. This research aims to provide a comprehensive review of the challenges associated with the implementation of blockchain technology in the IoV context.**

Keywords—Internet of vehicles (IoV); traffic congestion; smart sensors; connected vehicles; data privacy; data security; blockchain technology

I. Introduction

With the rapid development of the automobile industry, the Internet of Vehicles (IoV) technology is expected to grow as the most promising solution to ensure road safety and efficiency. However, this growth has brought numerous challenges regarding data storage, processing power, and data privacy and security. Traditionally, IoV data is all stored in a central node, where all network communication passes through, putting the security of the IoV network at serious risk because an attack on the central node would compromise all nodes in the network. Additionally, a centralized approach cannot handle real-time responses efficiently due to dynamic and large IoV scenarios.

Blockchain technology, originally developed for the cryptocurrency Bitcoin, ensures secure, trustworthy, and reliable transaction sharing among users based on peer-to-peer networks. As a decentralized approach, blockchain offers a transparent and secure exchange of information in the IoV network. Its decentralized and distributed architecture has demonstrated great ability in storing and processing big data while preserving the privacy and security of information. By combining the IoV with blockchain technology, security and privacy issues can be addressed. However, a blockchain-based IoV network still faces many obstacles, such as resource deficiency and large and dynamic IoV scenarios.

This paper proposes a contribution based on a systematic review methodology to address the challenges facing the blockchain-based IoV network. The methodology section explains the method used to search and select articles, the challenges associated with the blockchain-based IoV section focuses on analyzing the selected articles, and the results and important discoveries section presents a classification of the preceding challenges and highlights important observations. Finally, the conclusions and future directions section provides insights on the potential of blockchain in securing information exchange in IoV networks.

II. Background

A. Blockchain Architecture

A blockchain is a sort of distributed ledger technology (DLT) that comprises of a sequence of data containers called blocks. Where each block is containing a complete list of transaction information. Furthermore, each block is linked to the previous block by containing its hash value, and since each block is linked to the previous one, they then create a sequence of blocks called blockchain. Fig. 1 illustrates an example of a blockchain.

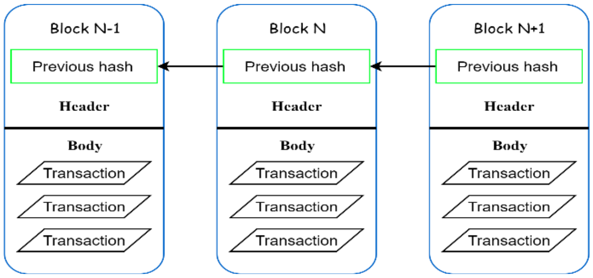

Fig. 1. Example of a blockchain.

1) Block: As predefined, blocks are data containers that consist of a block header and a block body. The header of the block contains valuable information required for its identification within the network. Each block header contains the following information:

- Block Version.
- Hash value of the previous block.
- The hash value associated with of all transactions recorded in this block, known as Merkle root hash.
- nBits, which represents the difficulty with which the current block was created.

- Timestamp.
- A random number which increases every hashing calculation known as Nonce.

As for the block body, it contains all transactional information which occurred in this block.

2) Transactions: Transactions are the most important part of blockchain, the whole blockchain ledger is designed to ensure a successful creation of transactions, and then move to spreading these transactions through the network to be validated by the other nodes. A transaction combines three key values, recipient address, sender information, and transaction record. That after being validated, gets added to the global blockchain as a new block.

3) Consensus: Once a new block is created, it must be validated by all nodes in the blockchain distributed ledger. This process is referred to as "consensus making." Depending on the blockchain and its use, there are several types of consensus algorithms that vary in terms of energy consumption, security, and scalability, but serve the same purpose of verifying that transactions are accurate and authentic. Some of the most commonly used consensus algorithms are proof of work (PoW), which is used with Bitcoin, and proof of stake (PoS), which is more energy-efficient.

"Mining" (proof of work) is a well-known process responsible for adding a new block to the blockchain ledger, distributed among all blockchain users. Participants in this process are called "miners." Mining involves solving a highly complex mathematical problem, which requires a large amount of time and energy, in order to find the correct hash. Miners try to solve this problem using powerful computers, and the first computer to find the correct hash receives the new block.

Proof of stake (PoS) techniques require "validators" to store and hold tokens in exchange for the right to collect transaction fees. PoS reduces the computational effort required to validate blocks and transactions. Proof of work ensures the security of the blockchain, while proof of stake changes the way blocks are confirmed by leveraging the computing resources of currency owners, requiring less computational effort. Owners stake their currency for the opportunity to validate blocks and become validators.

1) IoV architecture: Internet of vehicles (IoV) is a network connecting cars, pedestrians, and road infrastructure, through a process of information exchange. The network is equipped with a variety of sensors, which are responsible for collecting data from surrounding environments, to be shared with other parts of the network through the internet. IoV aims to enhance traffic conditions and reduce accidents and traffic congestion through interconnectivity. Fig. 2 illustrates IoV network structure. IoV architecture is composed of three main layers:

2) Perception layer, which englobes all vehicular sensors and devices required to collect environmental data. It also contains every hardware device required for the network functioning.

3) Network layer. This layer is responsible for data transmission among IoV devices through network connectivity. The most known networks for supporting these transmissions are Wi-FI, 4G/5G, and Wlan.

4) Application layer, is the layer responsible for data storage, data analysis, and decision-making regarding safety measures, in case of urgent traffic conditions. And in the case of autonomous driving cars, this layer controls the brakes, accelerator, and the engine, based on traffic conditions information received from different sensors in the network.

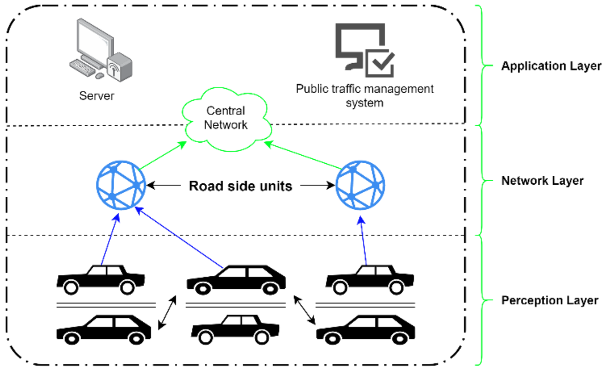

Fig. 2. IoV Structure.

III. Systematic Review Methodology

This research aims to answer the following question: what are the security limitations of the application of blockchain technology in IoV? This research question was the main subject of the analysis methodology of different research articles on the application of blockchain technology in IoV. It was used to select, filter, evaluate these studies, and exploit their results.

1) Search method: A systematic review regarding the application of blockchain technology in IoV was conducted using Scopus, Web of Science, and IEEE Xplore. To find relevant information on the subject, this combination of keywords was used (“data privacy and security”, “blockchain”, and “IoV”). Relevant scholarly articles were identified and selected to move forward in this review of the literature.

2) Criteria: Only the articles that fulfill the predefined criteria were considered, there are four key criteria that a study needs to achieve in order to be eligible, as shown in Table I.

TABLE I. Inclusion Criteria

No	Criteria
1	The study focused on blockchain-based IoV.
2	The paper discussed a security issue with the application of blockchain technology in IoV.
3	The proposed solution aimed to ensure data privacy and security in a blockchain-based IoV network.
4	Papers should be published recently.

3) Data collection: All information regarding the challenges, solutions, and results was extracted. The collected data from each paper was mainly about the security and privacy of exchanged information in a blockchain-based IoV network. However, some papers discussed other issues such as computing power, and handling dynamic and large IoV scenarios, which can cause a problem in achieving a secure and private exchange of information between vehicles, to this end we've decided to include these researches in our review in order to have a more exhaustive vision of the results Fig. 3.

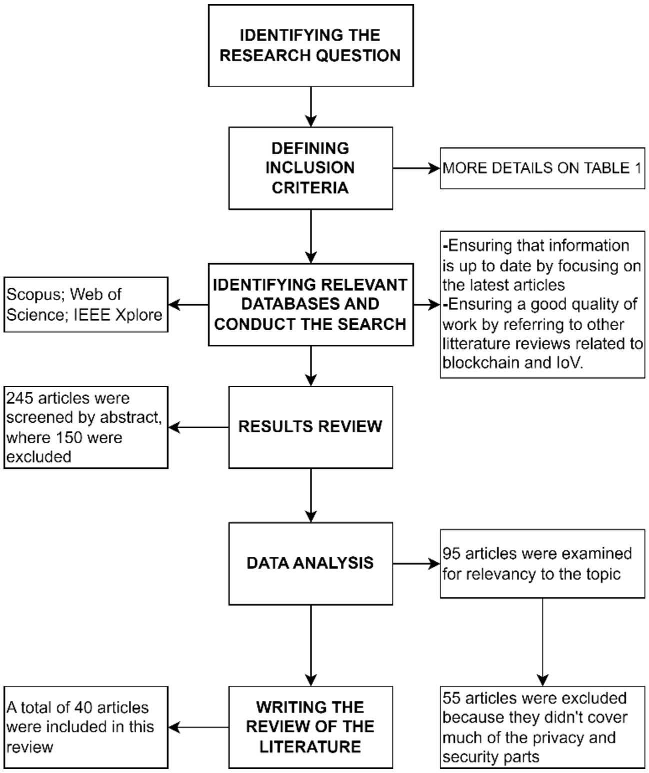
IDENTIFYING THE RESEARCH QUESTION
DEFINING INCLUSION CRITERIA
MORE DETAILS ON TABLE 1
IDENTIFYING RELEVANT DATABASES AND CONDUCT THE SEARCH
Scopus; Web of Science; IEEE Xplore
-Ensuring that information is up to date by focusing on the latest articles
-Ensuring a good quality of work by referring to other litterature reviews related to blockchain and IoV.
RESULTS REVIEW
245 articles were screened by abstract, where 150 were excluded
DATA ANALYSIS
95 articles were examined for relevancy to the topic
55 articles were excluded because they didn't cover much of the privacy and security parts
WRITING THE REVIEW OF THE LITERATURE
A total of 40 articles were included in this review

Fig. 3. Review process.

IV. The Challenges Associated with Blockchain-Based IoV

Our systematic review concerns a total of forty articles. The reviewed studies have shown a variety of limitations regarding the application of blockchain technology in IoV. These limitations should be examined in future studies on adopting blockchain technology as a solution to solve the security and privacy issues. As shown in Table II, more than half of the reviewed articles focused on solving the problem of security and privacy. However, other studies in this review that concentrate on other challenges, such as the security of smart sensors and resource limitations, were selected as well due to their impact on achieving a private and secure blockchain-based IoV network. The challenges associated with technological aspects are clearly dominating the article outcomes. The primary technology problems are identified as security, privacy, scalability, data collection, and security of smart sensors. It is worth noting that security, the driving force behind blockchain technology, is still a major concern for many academics. More information on these challenges, however, may be found in the challenges and results sections.

A. Security and Privacy

The growth of the Internet of Vehicles (IoV) has brought to light various challenges in regards to data storage, processing, and information privacy and security. In order to address these issues, Jiang, Fang, and Wang in [7] utilized blockchain technology in their implementation of IoV. The authors simulated the network's communication performance using MATLAB and found that under traffic congestion, the number of retransmissions increases, potentially leading to switching to a cellular network. However, the study does not take into account the impact of car traffic or the reliability of cellular networks. Vehicles in the IoV network communicate through third parties, which increases the risk of rogue cars transmitting false data. As a result, authentication of vehicles and service providers is crucial to prevent this issue. However, the authentication process involves exposing the vehicle's identification, and compromising privacy. Sharma and Chakraborty in [19] proposed a blockchain-based architecture (BLOCKAPP protocol) to address this challenge, which reduces the number of verifications and increases transaction rate by issuing pseudo-IDs to each vehicle. Wang, Zeng, Patterson, Jiang, and Doss in [23] studied the use of a blockchain-based authentication technique for IoV networks. The simulation results showed that this approach can handle information exchange, authentication, and encryption while being secure against malicious attackers. However, significant packet loss was observed during car registration and key distribution processes. Securing the IoV network becomes more challenging as the network becomes larger and more dynamic. To address this issue, a secure architecture based on blockchain technology was proposed in [15]. The framework allows for knowledge exchange among vehicles while maintaining privacy and security. The study used distributed smartphone applications and OBD-II to gather data and save it in the blockchain. The results showed that the framework can handle a high amount of concurrent traffic, but there were still some observed packet losses due to connection challenges. Narbayeva, Bakibayev, Abeshev, Makarova, Shubenkova, and Pashkevich in [14] focused on improving IoV cybersecurity through the use of blockchain technology. The authors utilized blockchain to create a secure system that provides parameters about a car through signals from nearby vehicles, and to track the movement of cars using the Exonum platform. However, this technique still relies on users being careful with their private keys.

TABLE II. CATEGORIES OF RELEVANT STUDIES

Aspects	Challenges	Description	Reference
Technological	Security and Privacy	Maintaining a secure and private exchange of information among vehicles	[1-2-3-4-5-6-7-8-9-10-11-12-13-14-15-16-17-27-28-29-30-31-32-33-34-35-36-37-38-39-40]
	Scalability	Blockchain's lack of scalability in case of huge amount of data	[18-19]
	Data collection	Enhancing the process of data collection	[20,14]
	Smart Sensors	Securing smart sensors against malicious attacks	[21,22]
Energetical	Resource limitations in the light of a high network performance	Analysis to enhance network performance, while respecting limited resource allocation	[23-24-25-26]

Due to the variety of security standards, the exchange of shared information between vehicles faces several security challenges. The use of blockchain technology can enhance the security of information exchange, however, it is still vulnerable to malicious attacks at higher layers and applications. Researchers Gunasekaran Raja et al. in [16] attempted to address the security flaws of blockchain by applying an AI-powered blockchain to Internet of Vehicles (IoV). The suggested system was evaluated by comparing it to traditional blockchain smart contracts, and the results showed that the smart contract vulnerabilities resulted in a significant cost for the system. Additionally, advancements in technology may pose a threat to the entire network. On the other hand, AI-powered intelligent contracts have a self-learning capability, allowing the system to improve its security. The study found that AI-powered intelligent contracts performed better in terms of preserving blockchain characteristics compared to blockchain smart contracts. Pranav Kumar Singh et al. in [21] addressed the same issue by combining AI and blockchain. However, the security of the system may be compromised by malicious or rogue nodes in the network. AI, with its predictive capability based on machine learning algorithms, is an effective solution for dealing with rogue nodes. It can quickly detect malicious peers, but there have been no real-world tests to evaluate the performance of the proposed framework. Jiawen Kang et al. in [8] proposed a soft security enhancement solution, which involves miner selection based on a reputation voting scheme, and block verification by standby miners using contract theory. The results of the simulation showed that the proposed approach outperforms traditional reputation schemes in detecting malicious miner candidates and increases shared information security. On the other hand, other researchers used a Byzantine consensus algorithm based on time sequence and gossip protocol (BCA-TG), on top of blockchain technology, to enhance the security of communication, consensus, and authentication of nodes in an IoV network [6]. The simulation results showed that consensus can be reached when the number of Byzantine nodes is less than half of the total number of nodes in the network. However, further testing needs to be done in real-world systems with a larger number of nodes and dynamic IoV scenarios.

One of the significant limitations in the Internet of Vehicles (IoV) network is the spectrum sensing process and ensuring a secure flow of information without interference. In case of a vehicle attack, the Cognitive Radio Network (CRN) can enhance decision-making in the IoV network. However, even though CRN has its benefits, network performance can be affected if malicious attackers modify data. To enhance network performance, a study by Geetanjali Rathee et al. suggested implementing a blockchain approach in CRN-based IoV to allow vehicles to keep track of all network operations and detect untrusted devices using the Technique for Order Preference by Similarity to Ideal Solution (TOPSIS) mechanism. According to simulation data, this method improves attack detection by 70%. However, the study did not address the authentication concerns in the TOPSIS method, and only a limited number of factors were evaluated in improving the spectrum sensing process and information transmission between vehicles. Another study by Yonggang Xiao et al. aimed to address the issue of safe information transmission between cars by building a rapid false news detection framework that uses edge computing and blockchain to identify fake news and prevent the exchange of any questionable information. The simulation results suggest that the proposed framework can provide accurate information about ongoing traffic events one minute after it starts and 4 minutes after the incident. However, the study did not address the issue of load balancing, and the framework has not been tested in a real-world setting. A study by Song-Kyoo Kim aimed to prevent network breakdown due to malicious attacks by designing a secure connected car network using a Blockchain Governance Game (BGC). BGC has been mathematically proven to be a robust model for defending systems from malicious attacks. However, there was no mention of simulation experiments in this study. Leo Mendiboure et al. focused on addressing security challenges in IoV using Software-Defined Networking (SDN) and regulating application identity and behavior using blockchain technology. This study did not contain any information on the simulation environment or findings, and various issues with the theoretical solution were raised. Another study by Saltanat Narbayeva et al. focused on safeguarding data transmission between vehicles using a hierarchical blockchain framework. According to simulation findings, blockchain was able to protect the network from rogue cars. However, the overhead and transactional throughput of the proposed framework were not studied, and there was no simulation in a real-world setting. The centralized approach no longer meets the requirements of knowledge exchange among intelligent cars due to the fast growth of information technology. With the advent of IoV technology, a more advanced intelligent transportation system may be realized. However, IoV still faces challenges such as handling diverse situations and failure tolerance. On the other hand, the centralized approach is considered weak due to its lack of flexibility and vulnerability to a single point of failure. Blockchain technology can address this issue, but it is difficult to determine the appropriate blockchain settings due to the unpredictable vehicle density. To solve this issue, Liming Gao et al. proposed a multichannel blockchain scheme that can select the best parameters based on the vehicle density.

A major challenge in a blockchain-based Internet of Vehicles (IoV) network is balancing privacy protection with information availability. Vehicles gather and share traffic data, and there is a risk of conflicts between this shared information. To mitigate this, a semi-centralized approach based on blockchain was suggested by Lichen Cheng et al. in [2]. This approach regulates traffic lights to guarantee efficient traffic flow while protecting shared information and the users' identities. However, this mode requires reducing interaction and encryption computation costs. The rapid increase in automobiles has led to the overuse of spectrum resources. To address this, a multiuser k-anonymous location protection method was proposed by Hongning Li et al. in [11]. The system preserves users' location privacy by creating anonymous zones and encouraging primary users to share spectrum. In [27], Zhang et al. proposed a blockchain-based solution for secure and privacy-preserving data sharing in the IoV. They analyze the challenges of privacy and security in the IoV and introduce a framework that includes privacy-preserving and secure data sharing. The framework was evaluated and shown to be effective in securing and preserving data privacy in the IoV environment. Hu and Li in [28] reviewed the security challenges in the IoV and discussed how blockchain technology can be used to address these challenges. They presented an overview of the IoV architecture and highlighted the security problems that exist in the data collection, storage, and transmission phases of IoV. They also described the characteristics of blockchain technology that make it suitable for use in the IoV and discussed existing blockchain-based solutions for securing IoV data. Tang, Wang, and Su in [29] proposed a secure and efficient communication scheme for the IoV based on blockchain technology. The proposed scheme uses a blockchain-based consensus algorithm to ensure data communication security in the IoV and a multi-layer encryption mechanism to protect data privacy. Simulation experiments showed that the proposed scheme was secure, efficient, and capable of meeting the communication requirements of the IoV. Iqbal, Liu, Guo, and Zhang in [30] proposed a blockchain-based trust management framework for the IoV. The framework uses blockchain technology to establish a trust mechanism that enhances the security and privacy of data transmission in the IoV. The performance of the framework was evaluated through simulation experiments, which showed that it effectively enhanced the security and privacy of data transmission in the IoV. Finally, Yang, Yang, and Huang in [31] presented an overview of the challenges and opportunities of using blockchain technology in the IoV. They analyzed the security and privacy problems in the IoV and discussed how blockchain technology can be used to address these challenges. They also described the architecture of a blockchain-based IoV system and highlighted the potential benefits of using blockchain in the IoV, such as increased data security and privacy.

Chen, X., and Li, Y. in [32] proposed a blockchain-based secure and privacy-preserving data sharing framework for the Internet of Vehicles (IoV). The authors aimed to address the security and privacy challenges associated with data sharing in the IoV by utilizing blockchain technology. The proposed framework comprised a data sharing process that utilized a smart contract to ensure data authenticity and integrity, as well as a privacy-preserving mechanism that used homomorphic encryption to protect the privacy of the data. The authors evaluated the proposed framework through a simulation experiment, which showed that it could effectively improve the security and privacy of data sharing in the IoV. Wang, X., Huang, Y., and Lu, R. in [33] proposed a blockchain-based secure data sharing framework for the Internet of Vehicles (IoV). The authors aimed to address the security and privacy challenges of data sharing in the IoV by utilizing blockchain technology. The proposed framework included a consensus mechanism and a smart contract to guarantee the authenticity and integrity of the data, as well as a privacy-preserving mechanism that used homomorphic encryption to protect the privacy of the data. The authors evaluated the proposed framework through a simulation experiment, which showed that it could effectively enhance the security and privacy of data sharing in the IoV. Zhang, Y., Yang, X., Yang, Y., and Huang, X. in [34] proposed a secure and privacy-preserving data sharing framework for the Internet of Vehicles (IoV) based on blockchain technology. The authors aimed to tackle the security and privacy challenges of data sharing in the IoV by using blockchain technology. The proposed framework consisted of a consensus mechanism and a smart contract to ensure the authenticity and integrity of the data, as well as a privacy-preserving mechanism that used homomorphic encryption to protect the privacy of the data. The authors evaluated the proposed framework through a simulation experiment, which showed that it could effectively improve the security and privacy of data sharing in the IoV. Zhang, Y., and Li, J. in [35] focused on applying blockchain technology to secure and privacy-preserving data sharing for the Internet of Vehicles (IoV). The authors proposed a blockchain-based framework for secure and privacy-preserving data sharing in the IoV, which could effectively secure and protect the privacy of the data shared by vehicles. The framework provided a secure and privacy-preserving platform for IoV applications and services, enabling trustworthy and secure data sharing among different parties in the IoV. The authors also analyzed the security and privacy of the proposed framework through experiments and simulations, demonstrating the effectiveness and feasibility of the framework in the IoV. Fang, S., Liu, X., and Wang, S. in [36] conducted a study that focused on the application of blockchain technology to secure data sharing in the Internet of Vehicles (IoV). The authors proposed a secure data sharing mechanism that utilized blockchain to guarantee data privacy and security in the IoV. They presented a prototype system to demonstrate the feasibility of their proposed solution. The results showed that their proposed system was effective in terms of data security and privacy protection in the IoV. Li, H., Li, H., and Lu, R in [37] focused on using blockchain to secure data sharing in the Internet of Vehicles. The authors presented a blockchain-based secure data sharing framework for the IoV, which aimed to protect the privacy and security of data in the IoV. The framework consisted of several components, including a data storage layer, a consensus layer, and a privacy protection layer. The authors evaluated the performance of their proposed framework, and the results showed that it was efficient and effective in terms of security and privacy

B. Scalability

With Bitcoin's dominance in the cryptocurrency market, scalability issues related to blockchain technology have come to the forefront. Articles have analyzed various critical criteria to assess Bitcoin's scalability, including maximum throughput and latency, which significantly impact the user experience. However, the transaction throughput receives the most attention, with reports indicating that Bitcoin has a maximum transaction throughput of only 7 transactions per second, which is low compared to other technologies. As a result, blockchain may not be able to support large-scale transactions. Blockchain is a novel technology that enables secure transactions between parties in a decentralized and transparent network. However, besides scalability and latency, it also faces the challenge of high energy consumption [10]. In the Internet of Vehicles (IoV) network, a large amount of data is collected to improve traffic safety, and blockchain's scalability limitations become a significant issue when dealing with big data [10]. To address this issue, some articles have proposed a Deep Reinforcement Learning (DRL) based performance optimization framework for blockchain-based IoV, which aims to optimize transactional throughput while preserving network latency and privacy [12].

C. Data Collection

Data collection in the Internet of Vehicles (IoV) is crucial for achieving its goals. However, this process is hindered by a major issue: the reluctance of vehicles to participate in sensing operations. Additionally, some sensing tasks may arise unexpectedly, placing a strain on the resources of a single vehicle. As a result, it is necessary to have a large number of vehicles participate. To address this challenge, a novel paradigm of two vehicles collaborating was proposed in [26]. This strategy is based on a bidding process that incentivizes vehicles to collaborate and share resources. In case of an emergency task, a time-window-based mechanism for task management among vehicles is used to increase vehicle involvement. Moreover, a blockchain architecture is utilized to secure data sharing through smart contracts. According to simulation studies, the processing time decreases as the number of vehicles increases.

Haoye Chai, Supeng Leng, Yijin Chen, and Ke Zhang in [1] aimed to improve the data collection process by incorporating Artificial Intelligence (AI) to help vehicles learn from their surroundings using a federated learning algorithm based on machine learning. The simulation results showed that the proposed algorithm is 10% more accurate than conventional federated learning algorithms. However, the overhead and transactional throughput of the proposed framework were not studied, and there was no simulation conducted in a real-world setting.

D. Security of Smart Sensors

The Internet of Vehicles (IoV) employs various smart sensors that are vulnerable to malicious attacks, which could compromise network security. To address this issue, Anastasia Theodouli, Konstantinos Moschou, Konstantinos Votis, Dimitrios Tzovaras, Jan Lauinger, and Sebastian Steinhorst in [22] focused on securing software updates for smart sensors, as an incorrect update could lead to incorrect data being generated on the network.

This study proposed a blockchain-based system for managing identity and trust across the entire IoV network with the aim of securing the update process. On the other hand, Geetanjali Rathee, Ashutosh Sharma, Razi Iqbal, Moayad Aloqaily, Naveen Jaglan, and Rajiv Kumar in [18] provided a blockchain infrastructure to protect smart sensors from malicious intrusions.

E. Resource Limitations in the Light of a High Network Performance

In a blockchain-based Internet of Vehicles (IoV), reaching consensus requires a high level of computational power, which some IoV nodes may not be able to support. To address this issue, Liya Xu, Mingzhu Ge, and Weili Wu in [25] proposed integrating edge computing into the blockchain-based IoV by installing roadside units as edge servers. They used an algorithm to simulate the IoV environment and found that additional factors, such as transmission distance, can impact the edge servers. Meanwhile, Liming Gao, Celimuge Wu, Zhaoyang Du, and others in [3] focused on resource management by using a hierarchical resource scheduling approach for the blockchain-enabled IoV. Their proposed scheme was tested using the Hyperledger Fabric platform, and the results indicate its promise. However, as blockchain is a relatively new technology, there is no suitable instrument for testing its performance in an IoV simulator, so only changes in network workload can be tracked. Artificial Intelligence (AI) has been utilized to handle IoV problems and manage its infrastructure, but this requires computing resources and accurate data. Without these, deploying AI could put the entire infrastructure at risk. Moreover, installing both blockchain and AI would consume a significant amount of IoV resources. To address this challenge, Ahmad Hammoud and his colleagues in [5] presented a Vehicular Edge Computing-based architecture that aims to deploy both AI and blockchain technologies while mitigating resource constraints. Despite its benefits, the architecture faces several challenges, such as increased demand on processing and storage resources during traffic congestion and imbalanced network congestion causing uneven data loads on different fog servers. Additionally, updating AI models across multiple servers may cause inconsistencies, and updating blockchain ledgers may be difficult due to the large number of transactions required. To solve this energy problem, Vishal Sharma in [20] proposed an efficient approach that regulates the number of transactions via distributed clustering, which was found to be 40% more energy-efficient than standard blockchain and 82% more efficient in terms of transactions. However, this proposed model has not yet been tested in a real-world setting.

V. Results and Important Discoveries

The purpose of this study was to review published articles that investigate the use of blockchain technology in the Internet of Vehicles (IoV). This review evaluated the existing deficiencies in the proposed solutions for ensuring privacy and security in the IoV network using blockchain technology, and provided practical suggestions for improving privacy and security while considering computational power and resource consumption. The following patterns were identified:

- The use of a DRL-based performance optimization framework to tackle the scalability issues in blockchain technology.
- The application of edge computing and distributed clustering to manage network resources.
- The integration of AI technology to strengthen the security of blockchain-based IoV network through the use of Byzantine consensus algorithms (BCA-TG) and blockchain governance game (BGC).
- The use of AI technology in the sensing process to improve vehicle data collection through federated learning algorithms.

Security and privacy are the primary challenges in the IoV network, as connected vehicles face difficulties in securely exchanging information and preserving user privacy. The review showed that the proposed solutions tend to converge towards using blockchain technology in IoV networks, but its limitations such as scalability, security issues, and high energy consumption require the use of other technologies along with blockchain to improve privacy and security.

AI technology was proposed to be used with blockchain to enhance network security, but still struggles with resource limitations. Distributed clustering and edge computing were proposed as solutions to the resource limitations, but emerging and unbalanced IoV scenarios such as congestion and accidents can increase data flow and consume more resources. A hierarchical resource scheduling scheme was also proposed to manage computing resources efficiently.

Moreover, the study addressed the growing consumption of spectrum resources in the automotive industry through a k-anonymous location protection scheme for multiuser. The review also emphasized the importance of securing smart sensors against attacks and highlighted the use of blockchain-based frameworks and quick fake news detection frameworks based on edge computing and blockchain to secure information exchange between vehicles. However, these solutions were not tested against emerging IoV scenarios and large load balancing.

VI. Conclusions and Future Directions

The significance of blockchain in ensuring the security of IoV networks has increased over the recent years. This research aims to provide a comprehensive overview of the challenges faced while adopting blockchain technology to secure IoV networks. A systematic review was carried out to assess the research topic "What are the difficulties in adopting blockchain for securing IoV networks?" as reported in the existing literature.

The difficulties encountered in adopting blockchain for IoV networks were categorized into three categories: security of smart sensors, security and privacy concerns, computing power and resource limitations. The findings of this research suggest that the use of blockchain technology alone is not sufficient to address privacy and security issues. However, integrating blockchain with AI technology has shown promise in enhancing the security of the network. Nevertheless, the integration still faces challenges such as resource limitations and infrastructure malfunctions. Therefore, future research should concentrate on combining AI technology with blockchain to improve privacy and security in IoV networks.

To tackle the issue of resource limitations, edge computing and distributed clustering appear to be effective in managing resources and reducing consumption. The scalability of the network, especially with the growing number of connected vehicles and dynamic IoV scenarios, should also be taken into consideration in future studies.

References

[1] Haoye Chai, Supeng Leng, Yijin Chen, and Ke Zhang. A hierarchical blockchain-enabled federated learning algorithm for knowledge sharing in internet of vehicles. IEEE Transactions on Intelligent Transportation Systems, 22(7):3975–3986, 2020.

[2] Lichen Cheng, Jiqiang Liu, Guangquan Xu, Zonghua Zhang, Hao Wang, Hong-Ning Dai, Yulei Wu, and Wei Wang. Sctsc: A semicentralized traffic signal control mode with attribute-based blockchain in iovs. IEEE Transactions on Computational Social Systems, 6(6):1373–1385, 2019.

[3] Liming Gao, Celimuge Wu, Zhaoyang Du, Tsutomu Yoshinaga, Lei Zhong, Fuqiang Liu, and Yusheng Ji. Toward efficient blockchain for the internet of vehicles with hierarchical blockchain resource scheduling. Electronics, 11(5):832, 2022.

[4] Liming Gao, Celimuge Wu, Tsutomu Yoshinaga, Xianfu Chen, and Yusheng Ji. Multi-channel blockchain scheme for internet of vehicles. IEEE Open Journal of the Computer Society, 2:192–203, 2021.

[5] Ahmad Hammoud, Hani Sami, Azzam Mourad, Hadi Otrok, Rabeb Mizouni, and Jamal Bentahar. Ai, blockchain, and vehicular edge computing for smart and secure iov: Challenges and directions. IEEE Internet of Things Magazine, 3(2):68–73, 2020.

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

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

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

[9] Song-Kyoo Kim. Enhanced iov security network by using blockchain governance game. Mathematics, 9(2):109, 2021.

[10] Akshay Kumaran, Amit Kumar Tyagi, and S Pradeep Kumar. Blockchain technology for securing internet of vehicle: Issues and challenges. In 2022 International Conference on Computer Communication and Informatics (ICCCI), pages 1–6. IEEE, 2022.

[11] Hongning Li, Jingyi Li, Hongyang Zhao, Shunfan He, and Tonghui Hu. Blockchain-based incentive mechanism for spectrum sharing in iov. Wireless Communications and Mobile Computing, 2022, 2022.

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

[13] Leo Mendiboure, Mohamed Aymen Chalouf, and Francine Krief. To- ´ wards a blockchain-based sd-iov for applications authentication and trust management. In International Conference on Internet of Vehicles, pages 265–277. Springer, 2018.

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

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

[16] Gunasekaran Raja, Yelisetty Manaswini, Gaayathri Devi Vivekanandan, Harish Sampath, Kapal Dev, and Ali Kashif Bashir. Ai-powered blockchain-a decentralized secure multiparty computation protocol for iov. In IEEE INFOCOM 2020-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), pages 865–870. IEEE, 2020.

[17] Geetanjali Rathee, Farhan Ahmad, Fatih Kurugollu, Muhammad Ajmal Azad, Razi Iqbal, and Muhammad Imran. Crt-biov: a cognitive radio technique for blockchain-enabled internet of vehicles. IEEE Transactions on Intelligent Transportation Systems, 22(7):4005–4015, 2020.

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

[19] 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.

[20] Vishal Sharma. An energy-efficient transaction model for the blockchain-enabled internet of vehicles (iov). IEEE Communications Letters, 23(2):246–249, 2018.

[21] Pranav Kumar Singh, Sukumar Nandi, Sunit K Nandi, Uttam Ghosh, and Danda B Rawat. Blockchain meets ai for resilient and intelligent internet of vehicles. arXiv preprint arXiv:2112.14078, 2021.

[22] Anastasia Theodouli, Konstantinos Moschou, Konstantinos Votis, Dimitrios Tzovaras, Jan Lauinger, and Sebastian Steinhorst. Towards a blockchain-based identity and trust management framework for the iov ecosystem. In 2020 Global Internet of Things Summit (GIoTS), pages 1–6. IEEE, 2020.

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

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

[25] Liya Xu, Mingzhu Ge, and Weili Wu. Edge server deployment scheme of blockchain in iovs. IEEE Transactions on Reliability, 71(1):500–509, 2022.

[26] Bo Yin, Yulei Wu, Tianshi Hu, Jiaqing Dong, and Zexun Jiang. An efficient collaboration and incentive mechanism for internet of vehicles (iov) with secured information exchange based on blockchains. IEEE Internet of Things Journal, 7(3):1582–1593, 2019.

[27] Zhang, Y., Chen, X., & Li, J. (2020). Blockchain-based secure and privacy-preserving data sharing for Internet of Vehicles. IEEE Transactions on Industrial Informatics, 16(8), 5497-5507.

[28] Hu, M., & Li, M. (2019). A review of security issues in Internet of Vehicles and blockchain-based solutions. Journal of Ambient Intelligence and Humanized Computing, 10(5), 7947-7962.

[29] Tang, Z., Wang, C., & Su, J. (2019). Secure and efficient communication in blockchain-based Internet of Vehicles. Sensors, 19(2), 410.

[30] K. Iqbal, Y. Liu, L. Guo, and J. Zhang, "A Blockchain-based Trust Management Framework for Internet of Vehicles," in IEEE Internet of Things Journal, vol. 5, no. 6, pp. 5586-5595, Dec. 2018.

[31] Yang, Z., Yang, J., & Huang, X. (2018). Blockchain in the Internet of Vehicles: challenges and opportunities. The Journal of Supercomputing, 74(9), 4670-4689.

[32] Chen, X., & Li, Y. (2019). Blockchain-based secure and privacy-preserving data sharing for Internet of Vehicles. In 2019 IEEE 21st International Conference on High Performance Computing and Communications; IEEE 17th International Conference on Smart City; IEEE 5th International Conference on Data Science and Systems (HPCC/SmartCity/DSS) (pp. 522-529). IEEE.

[33] Wang, X., Huang, Y., & Lu, R. (2018). Blockchain-based secure data sharing in Internet of Vehicles. In 2018 IEEE 19th International Conference on Intelligent Transportation Systems (ITSC) (pp. 485-490). IEEE.

[34] Zhang, Y., Yang, X., Yang, Y., & Huang, X. (2019). Secure and privacy-preserving data sharing in Internet of Vehicles based on blockchain technology. Journal of Network and Computer Applications, 137, 1-13.

[35] Zhang, Y., & Li, J. (2019). Blockchain-based secure and privacy-preserving data sharing in Internet of Vehicles. In 2019 IEEE 20th International Conference on High Performance Computing and Communications; IEEE 17th International Conference on Smart City; IEEE 5th International Conference on Data Science and Systems (HPCC/SmartCity/DSS) (pp. 2380-2386). IEEE.

[36] Fang, S., Liu, X., & Wang, S. (2018). Secure data sharing in Internet of Vehicles based on blockchain technology. In 2018 IEEE 20th International Conference on Computer Supported Cooperative Work and Social Computing (CSCW) (pp. 1145-1154). IEEE.

[37] Li, H., Li, H., & Lu, R. (2018). Blockchain-based secure data sharing in Internet of Vehicles. In 2018 IEEE Conference on Computer Communications (INFOCOM) Workshops (pp. 535-540). IEEE.

[38] Li, L., Li, J., Li, J., & Li, H. (2019). A blockchain-based secure and privacy-preserving data sharing framework for Internet of Vehicles. In 2019 IEEE 20th International Conference on Computer Supported Cooperative Work and Social Computing (CSCW) (pp. 911-920). IEEE.

[39] Zhang, Y., Chen, X., & Li, J. (2020). Blockchain-based secure and privacy-preserving data sharing in Internet of Vehicles. In 2020 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) (pp. 1686-1693). IEEE.

[40] Chen, X., & Li, Y. (2020). Blockchain-based secure and privacy-preserving data sharing in Internet of Vehicles. In 2020 IEEE 21st International Conference on High Performance Computing and Communications; IEEE 17th International Conference on Smart City; IEEE 5th International Conference on Data Science and Systems (HPCC/SmartCity/DSS) (pp. 2739-2746). IEEE.