Computer Systems
Science and Engineering

Tech Science Press

DOI: 10.32604/csse.2024.057754

ARTICLE

Revolutionizing Automotive Security: Connected Vehicle Security Blockchain Solutions for Enhancing Physical Flow in the Automotive Supply Chain

Khadija El Fellah[1,*], Ikram El Azami[2,*], Adil El Makrani[2], Habiba Bouijij[3] and Oussama El Azzouzy[4]

[1]Laboratory of Research in Informatics, Faculty of Science, Ibn Tofail University, Kenitra, 14000, Morocco

[2]Department of Informatics, Laboratory of Research in Informatics, Faculty of Science, Ibn Tofail University, Kenitra, 14000, Morocco

[3]SSLab ENSIAS, Mohammed V University in Rabat, Rabat, 10000, Morocco

[4]LIS Lab, Faculty of Science Ain-Chock, Hassan II University, Casablanca, 20000, Morocco

*Corresponding Authors: Khadija El Fellah. Email: khadija.elfellah@uit.ac.ma; Ikram El Azami. Email: ikram.elazami@uit.ac.ma

Received: 27 August 2024 Accepted: 08 November 2024 Published: 03 January 2025

ABSTRACT

The rapid growth of the automotive industry has raised significant concerns about the security of connected vehicles and their integrated supply chains, which are increasingly vulnerable to advanced cyber threats. Traditional authentication methods have proven insufficient, exposing systems to risks such as Sybil, Denial of Service (DoS), and Eclipse attacks. This study critically examines the limitations of current security protocols, focusing on authentication and data exchange vulnerabilities, and explores blockchain technology as a potential solution. Blockchain's decentralized and cryptographically secure framework can significantly enhance Vehicle-to-Vehicle (V2V) communication, ensure data integrity, and enable transparent, immutable transactions within the supply chain. Additionally, blockchain strengthens authentication, secures digital identities, and improves data sharing, reducing the risk of unauthorized access and data breaches. Our contribution lies in the proposal to integrate Artificial Intelligence (AI) with blockchain technology to further improve security by refining cryptographic methods, automating key management, and bolstering anomaly detection. Despite challenges related to computational complexity, latency, scalability, and regulatory concerns, the combination of blockchain, AI offers the transformative potential to enhance the security, transparency, and efficiency of connected vehicle systems and their supply chains.

KEYWORDS

Automotive supply chain; smart transportation; blockchain technology; connected vehicle; data security; physical flow; artificial intelligence (AI)

1 Introduction

With the rapid evolution of the Internet of Vehicles (IoV), ensuring secure vehicular communication has become critical for enhancing road safety and driving efficiency [1]. However, conventional vehicle key authentication systems, such as Public Key Infrastructure (PKI) and asymmetric key pairs, face significant security challenges [2]. These systems are vulnerable to various attacks, including

Sybil attacks, which involve forged nodes that disrupt genuine communication, leading to erroneous data transmission [3]; Eclipse attacks, where multiple nodes are compromised to gain control over communication channels, jeopardizing network integrity [4]; and Denial-of-Service (DoS) attacks, which overwhelm the network with excessive requests, causing delays for legitimate users and draining essential resources [5].

As the IoV expands, the increasing number of connected vehicles amplifies cybersecurity risks. Hackers exploit vulnerabilities to access sensitive data, with message injection attacks targeting Electronic Control Units (ECUs), leading to severe operational failures [6]. Additionally, location anomaly detection methods using Radio Access Network (RAN) data can identify potential hijacking attempts, enhancing overall vehicle security [7]. Real-world vulnerabilities, such as those discovered in Tesla vehicles, underscore the urgent need for multi-layered security systems to prevent exploitation [8].

Despite the growing recognition of these vulnerabilities, there is still a notable lack of in-depth research into how blockchain technology can effectively address security issues within the automotive industry. Blockchain, known for its secure, transparent, and decentralized method of conducting transactions, remains underexplored in the context of vehicle communications [9]. While traditional authentication systems face significant vulnerabilities, such as those exploited in Sybil and DoS attacks, there is insufficient research on how blockchain technology can specifically mitigate these risks in connected vehicle systems. Unlike traditional authentication systems, blockchain offers a decentralized solution to mitigate these vulnerabilities by validating transactions securely through cryptographic techniques [10]. Transactions between parties are recorded within blocks, making unauthorized data tampering and access difficult [11]. This is particularly critical in the automotive sector, where reliance on third-party intermediaries poses significant challenges to secure communication [12].

Smart transportation systems, which aim to optimize energy management through information exchange among autonomous vehicles, face significant challenges in ensuring high-quality service (QoS) in secure and reliable communication [13,14]. Blockchain technology has emerged as a potential solution for improving data security and privacy in-vehicle networks [1]. By enabling secure and reliable communication, blockchain strengthens the privacy and transparency of connected autonomous vehicles while minimizing transportation delays, contributing to a safer environment in smart cities [15].

Traditional authentication systems demonstrate considerable vulnerabilities, as evidenced by various studies. One comprehensive investigation revealed 4221 vulnerable instances of applications, with over 50% remaining exposed after four weeks, highlighting the prevalence of missing authentication vulnerabilities [16]. Additionally, a security analysis of popular authenticator applications found sensitive data, such as secret keys, stored in plain text, making them susceptible to attacks [17]. In Nigeria, Unstructured Supplementary Service Data (USSD) banking protocols showed weak authentication, with some services requiring no authentication at all [18]. These findings underscore the critical need for enhanced security measures in authentication systems, as attackers can exploit these weaknesses to gain unauthorized access to sensitive information.

Given these challenges, the need for robust, scalable solutions has never been more pressing. Blockchain technology has emerged as a promising solution for enhancing data security and privacy in-vehicle networks. By enabling decentralized authentication, blockchain reduces reliance on centralized systems, improving efficiency and security. It also enhances data integrity through immutable ledgers and improves privacy by protecting sensitive location data in vehicular networks. Furthermore, blockchain facilitates efficient and secure inter-vehicle communication, reducing latency and improving the Quality of Service (QoS) in smart transportation systems.

Blockchain offers significant advantages over traditional security methods, particularly in enhancing safety within connected vehicle systems. These advantages include enhanced data integrity through immutable records that are crucial for insurance and safety checks, real-time threat detection through vehicle authentication and alert systems, and improved trust and transparency among stakeholders, including insurance companies and vehicle owners [19–22].

However, challenges such as scalability and integration with existing systems remain critical considerations for the widespread adoption of blockchain in connected vehicle systems. While blockchain offers significant security advantages over traditional methods, its successful integration into existing systems and the automotive industry remains a research gap that needs addressing. This research explores how blockchain technology can improve safety in the automotive industry, particularly within connected vehicle systems.

By integrating blockchain with AI technologies, this study seeks to optimize real-time anomaly detection and enhance decision-making processes, addressing key limitations such as latency and scalability. The combination of blockchain and AI offers a powerful solution to the persistent cybersecurity challenges in IoV, ensuring faster response times, improved system performance, and enhanced privacy measures. This approach aims to establish a robust, multi-layered defense mechanism that ensures the highest levels of security for connected vehicles in future smart city environments.

2 Background of Research

2.1 Blockchain Technology Overview

Blockchain is a decentralized peer-to-peer system in which each participant maintains a copy of the ledger, eliminating single points of failure. It was originally developed to solve the problems associated with crypto-currencies [23], and it securely manages various data types. The ledger consists of blocks with two parts: the body, containing transactions like monetary exchanges and medical data, and the header, containing metadata such as timestamps and transaction hashes. This structure forms a linked chain, making falsification difficult as the chain lengthens [24]. Fig. 1 illustrates the architecture of the blockchain, showing how these blocks are interconnected and highlighting the importance of the hashes that link them together.

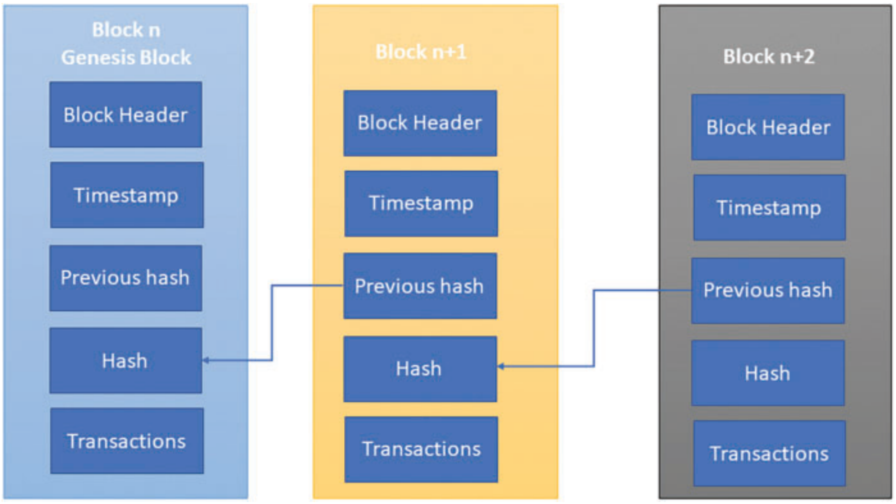

Figure 1: Blockchain architecture [25]

Blockchain includes public (permissionless) blockchains, accessible to everyone, and private (permissioned) blockchains, requiring authorization. Its main characteristics are immutability, decentralization, and the permanence of validated transactions. It offers partial anonymity for transaction participants and uses algorithms for traceability, ensuring a secure, decentralized, and transparent platform [26].

Two key components of blockchain technology significantly enhance its functionality: cryptography and smart contracts.

- **Cryptography** is fundamental to blockchain security. It uses algorithms to encrypt data, ensuring that information is stored securely and only accessible to authorized parties. Each transaction is digitally signed using a pair of cryptographic keys (public and private), enabling participants to confirm the authenticity of transactions. While preserving the confidentiality of sensitive information. This mechanism not only strengthens the integrity of the blockchain but also preserves the privacy of users [15].

- **Smart contracts** are automated contracts that have their terms and conditions coded directly into the software. They run on the blockchain and automatically execute and enforce the conditions when certain conditions are met. This means that intermediaries are no longer needed. This process increases efficiency, reduces costs, and improves transparency since all participants can independently verify performance. Moreover, once deployed, smart contracts are immutable, offering higher security for the transactions they manage [27].

By integrating the elements of blockchain, cryptography, and smart contracts, businesses within the automotive sector can substantially enhance their operations, particularly in the real-time tracking of vehicles and components throughout the supply chain. This technological convergence optimizes logistics and inventory management efficiency, safeguards sensitive information, and enhances transparency. In the context of connected vehicles, these solutions strengthen security measures, protect against data tampering, and facilitate safer interactions between vehicles, manufacturers, and consumers.

2.2 Connected Vehicle Overview

The Internet of Vehicles (IoV), or connected vehicle concept, refers to vehicles equipped with internet connectivity that utilize Vehicular Ad-hoc Networks (VANET) technology [28]. This advanced integration allows for the real-time transmission of crucial safety data among vehicles, thereby significantly enhancing the driving experience by optimizing safety and efficiency. Recent developments in this field are increasingly focused on the application of blockchain technology in the automotive sector. This technological shift aims to improve the traceability and management of vehicle flows and automotive parts [29].

Blockchain technology is celebrated for its robust security and reliability in data handling. It operates by recording and distributing data across a network, effectively eliminating the risks of duplication or tampering. The key features that make blockchain an innovative solution in the automotive sector include its cryptographic security measures, consensus mechanisms, and immutable nature, ensuring that recorded data cannot be changed retroactively [29].

Furthermore, blockchain's decentralized architecture removes the need for a central authority, enhancing transparency and user trust. These attributes are key to transforming the way vehicle data is managed, making processes more secure, transparent, and efficient [30].

By integrating blockchain with IoV, businesses can achieve real-time tracking of automotive components, streamline operations, and bolster the security of sensitive data exchanges. Fig. 2 illustrates the IoV or connected vehicle blockchain, highlighting its integration and functionality within the automotive ecosystem.

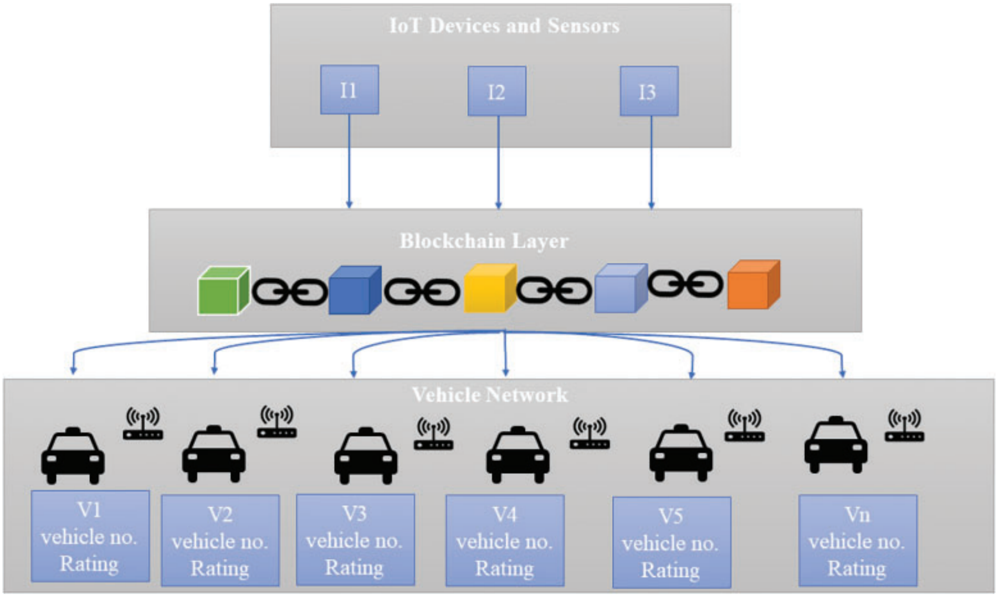

Figure 2: IoV or connected vehicle blockchain [31]

3 Related Work

The integration of blockchain technology into the automotive supply chain has received particular attention due to its potential to improve road safety and driving efficiency. As a result, with the rise of the Internet of Vehicles (IoV) and the increasing number of connected vehicles, cybersecurity risks have become more significant, exposing traditional vehicle key authentication systems to attack [6].

Common threats such as Sybil, Eclipse, and denial-of-service attacks compromise the security of communications in-vehicle networks. Research has highlighted the limitations of current authentication methods for ensuring secure communications. For instance, Karl et al. identified vulnerabilities in over 50% of popular authentication applications, which remained exposed for long periods, posing serious security risks [16]. Nash et al. found that sensitive information such as secret keys was stored in the clear, demonstrating the need for more stringent security measures [17].

In the context of connected vehicles, this vulnerability poses serious risks, as the storage and transmission of sensitive vehicle data must be properly protected. Blockchain solutions can play a key role here, offering immutable records and secure data encryption to mitigate these risks and enhance the security of the automotive supply chain.

Blockchain solutions can play a key role here, offering immutable records and secure data encryption to mitigate these risks and enhance the security of the automotive supply chain. Blockchain technology, renowned for its secure, decentralized transaction systems, has been explored as a solution to these challenges. Blockchain reduces the risks associated with data tampering and unauthorized access by eliminating the need for third-party intermediaries, which are common in traditional systems.

Blockchain is therefore a promising tool for improving the security of connected vehicles. Blockchain is therefore a promising tool for improving the security of connected vehicles.

While Yadav et al. demonstrated blockchain's ability to create immutable records for insurance and security checks, real-time communication and security within connected vehicle systems remain underexplored [20]. Gaba et al. highlighted blockchain's potential for real-time threat detection, but their research did not address how artificial intelligence (AI) could enhance blockchain-based cryptographic practices and automate key management [32].

This research builds on previous work by proposing an innovative integration of AI and blockchain. Unlike previous studies that have focused on traditional authentication vulnerabilities, this research examines the combined effects of AI and blockchain, improving real-time data sharing, decision-making, and operational efficiency in connected vehicle systems. This approach not only strengthens encryption methods but also enables anomalies to be detected more quickly, an area that has been little explored until now.

Previous research, such as Viswanadham et al., has focused on blockchain's role in vehicle authentication and data sharing. However, issues of scalability and interoperability have often been overlooked [22]. This work addresses these challenges, particularly in terms of real-time communication and transaction processing in connected vehicle ecosystems, which face critical concerns about latency and power consumption.

Although blockchain has been shown to improve trust in vehicle authentication and traceability, the need for comprehensive regulatory frameworks to support large-scale adoption remains largely unmet. This research calls for the development of such frameworks, as legal and privacy concerns are barriers to large-scale implementation in connected vehicle systems.

3.1 *Comparative Analysis of Recent Studies*

Recent studies have shown that blockchain can significantly improve security, privacy, and trust in IoV systems. In 2024, Yadav et al. proposed a blockchain-based trust model to improve data integrity and reliability in vehicle-to-vehicle communications. Although their model addresses vulnerabilities in vehicle-to-vehicle communication, some security flaws remain, particularly in managing real-time interactions [20].

Similarly, in 2024, Hussain et al. have investigated blockchain for enhancing trust and access control in IoV, focusing on decentralized systems [33]. However, while their framework improves decentralized access, it is still limited to real-time vehicle interactions. Building on this, in 2023, Castillo et al. have introduced a decentralized simulation workflow to test security protocols in connected vehicles, but their approach faces challenges, as the simulation relies on non-representative datasets, suggesting the need for more comprehensive testing [19].

In addition to these efforts, studies such as Azath et al. and Verma et al. focused on blockchain's ability to identify malicious nodes and enhance data integrity within vehicular networks [21]. These efforts demonstrated blockchain's potential but also revealed limitations in scaling solutions for large IoV networks and managing trust effectively.

A comparative analysis of these studies reveals that while blockchain enhances the security of vehicle-to-vehicle communications and trust in IoV persistent challenge such as performance and privacy concerns—continue to affect scalability. Therefore, Research gaps remain regarding the scalability and computational load of blockchain solutions in large, dynamic IoV ecosystems. Future work should focus on refining test environments, improving real-time interactions and resolving scalability and privacy issues to fully exploit the potential of blockchain in connected vehicles.

4 Methodology

The main objective of this study is to examine the main features and functions of blockchain technology, in particular its contribution to improving safety and logistics in the automotive supply chain, with a specific focus on connected vehicles. The study is guided by the following research questions:

- How can blockchain technology enhance the safety and efficiency of the automotive supply chain?
- What are the principal security threats within the current automotive supply chain, and how can blockchain help mitigate these risks?
- What are the concrete challenges and advantages of combining blockchain and connected vehicle technology in the supply chain?

Data Collection: We conducted an extensive literature review, collecting all relevant articles published between 2018 and 2024 in leading databases such as Web of Science, Scopus, IEEE Xplore, ACM Digital Library, along with other significant academic publications. The initial search identified **150 articles**. After applying exclusion criteria and removing **duplicates**, **75 articles** were selected for detailed analysis, ensuring they were representative and relevant to blockchain's application in the automotive supply chain, especially concerning security and integration with connected vehicle technology.

Inclusion Standards and Search Query: This review examines literature focusing on the application of blockchain technology within the automotive supply chain. Emphasizing security and connected vehicle integration. The search query employed was **(Blockchain AND "automotive supply chain" AND "connected vehicle" AND "security")**. This search provided a comprehensive review of the relevant literature focusing on the intersection of these topics.

Exclusion Criteria: Articles that did not directly focus on blockchain technology, the automotive supply chain, or connected vehicle security were excluded. Additionally, we excluded articles published before 2018 to maintain relevance to the latest developments in the field.

Data Extraction: The information contained in the selected articles is systematically extracted using a predefined data extraction model. This model collects essential information, including the title, list of authors, publication year, research aims, methodology, findings, and limitations. Particular attention was paid to data points concerning blockchain implementation, security measures, integration with connected vehicles, and associated challenges. In addition, we recorded the total volume of data analyzed, including the number of articles reviewed, and noted any duplicates identified during the selection process.

Data Analysis: The extracted data underwent rigorous analysis using content analysis techniques. Key themes were identified and categorized through manual coding. Categories included:

- **Security Solutions:** How blockchain enhances security in automotive supply chains.
- **Blockchain Adoption Barriers:** Challenges encountered during implementation.
- **Integration Challenges:** Issues related to integrating blockchain with connected vehicle technology.

Key data points were evaluated based on their effectiveness, scalability, and implementation complexity, ensuring a structured comparison of findings. Articles were further assessed based on their citation impact and peer-review status to focus on high-quality and influential research.

Future Research Directions: This study suggests possible avenues for future research, particularly about the technical and regulatory challenges of implementing blockchain solutions in the automotive industry supply chain.

To improve the rigor and applicability of this study, we are in the process of incorporating empirical tests, simulations, and case studies in future phases.

Limitations: This study acknowledges several limitations, including:

- Accessibility and representativeness of the articles selected.
- Possible biases in literature analysis.
- The ability to generalize results to different segments of the automotive industry. By following this methodology, the study aims to propose a secure, scalable, and efficient blockchain-based solution that enhances the physical flow within the automotive supply chain while addressing challenges such as data integrity, security, and real-time management.

Fig. 3 represents the conceptual research design provides a framework for understanding the structure and direction of the study.

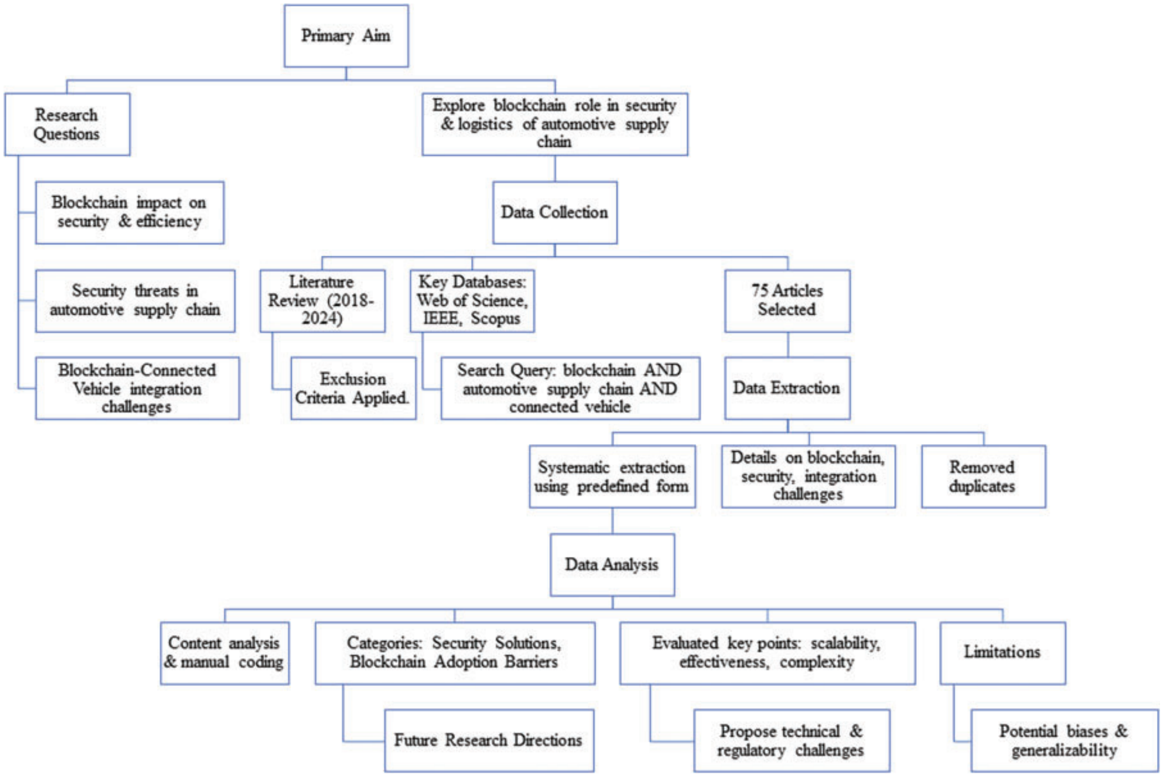
Primary Aim
Research Questions
Explore blockchain role in security & logistics of automotive supply chain
Blockchain impact on security & efficiency
Data Collection
Security threats in automotive supply chain
Literature Review (2018-2024)
Key Databases: Web of Science, IEEE, Scopus
75 Articles Selected
Blockchain-Connected Vehicle integration challenges
Exclusion Criteria Applied.
Search Query: blockchain AND automotive supply chain AND connected vehicle
Data Extraction
Systematic extraction using predefined form
Details on blockchain, security, integration challenges
Removed duplicates
Data Analysis
Content analysis & manual coding
Categories: Security Solutions, Blockchain Adoption Barriers
Evaluated key points: scalability, effectiveness, complexity
Limitations
Future Research Directions
Propose technical & regulatory challenges
Potential biases & generalizability

Figure 3: Conceptual research design

5 Research Findings

5.1 Approach to Analyzing and Classifying Results

In this chapter, we analyze blockchain-based solutions for the security of connected vehicles and their integration into the automotive supply chain. The findings are organized into three primary categories: security measures, integration with the automotive supply chain, and the enhancement of physical flow within the automotive supply chain. This organization was established through a systematic literature review and empirical studies, concentrating on the key themes recognized throughout the research process.

- **Security Features:** This section describes the various security protocols employed in blockchain technology to protect connected vehicles and ensure data integrity. The classification within this section was derived from analyzing different security frameworks and their effectiveness in real-world applications.

- **Integration with the Automotive Supply Chain:** Findings in this category emerged from case studies that illustrate how blockchain can be leveraged to streamline processes within the automotive industry. The results were categorized based on the degree of integration and the specific benefits observed in different supply chain scenarios.

- **Enhancing Physical Flow:** The analysis in this section focuses on how blockchain technology facilitates the physical flow of materials within the automotive supply chain. The results are organized according to the main improvements observed, such as increased transparency, trust, and efficiency in product movement. These results have been synthesized from case studies and a thorough review of existing literature, ensuring a comprehensive understanding of the effect of blockchain technology on vehicle safety and supply chain management.

Fig. 4 presents a conceptual mind map outlining the key elements needed to revolutionize automotive security, including AI integration, blockchain technology and future research, all aimed at improving security. The map explores aspects such as cryptographic security, supply chain integration, anomaly detection and quantum-resistant encryption. It also addresses challenges such as scalability, energy consumption and transaction latency, while highlighting the importance of regulatory frameworks and technical solutions for future progress.

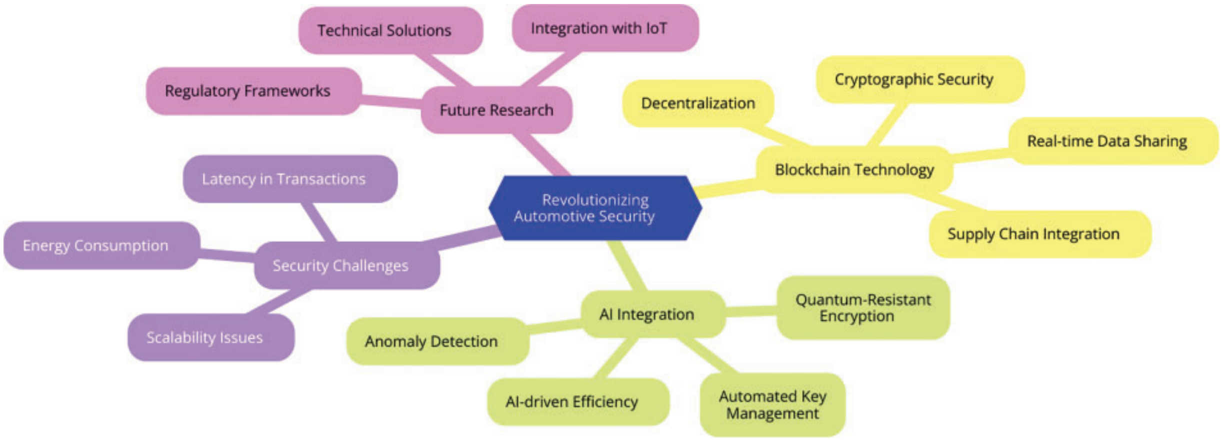

Figure 4: Transforming automotive security: conceptual mind map

5.2 Blockchain-Based Solutions for Connected Vehicle Security

Blockchain, recognized as a distributed and immutable ledger, has gained significant traction for ensuring data integrity, security, and resistance to tampering [34]. Its application in connected vehicle security offers an extension of existing solutions towards data provenance [35]. Within a blockchain system, data provenance and privacy are achieved through robust management of authentication and key provisioning, employing unique crypto fingerprints/key pairs (private and public keys) assigned to vehicles and associated data records [36].

Current advancements in the field primarily explore experimentation with local Proof of Work (PoW) or, more commonly, Proof of Elapsed Time (PoET) mechanisms, often relying on trusted Intel CPUs, as well as permissioned license-plate-based blockchain ledgers linked to vehicles via Dedicated Short-Range Communication (DSRC) or cellular connections [37]. Additionally, smart contracts linked to specific vehicle data are useful in blockchain-driven supply chain integrity management, streamlining leasing, and car maintenance services [38]. Blockchain is also adept at facilitating secure vehicular data sharing, mitigating challenges like tampering and privacy breaches [39].

Furthermore, blockchain technology can effectively protect user privacy and increase security in smart vehicles, benefiting users and reducing security threats [40]. A blockchain framework effectively protects connected and autonomous vehicles, offering a 79% success rate in preventing security issues like smart device compromise and user rating alteration [31].

5.2.1 Comparative Analysis of Cryptographic Algorithms and Blockchain Solutions

Recent research provides valuable insights into the performance and applicability of cryptographic algorithms and smart contracts in securing vehicular communication systems.

- **Performance Variability:** The efficiency of cryptographic algorithms can vary considerably depending on network conditions [41]. Symmetric algorithms, such as AES, RC6, and Blowfish, are recognized for their superior processing speed; however, they can present security risks compared to asymmetric algorithms such as Rivest–Shamir–Adleman RSA [42]. The RSA algorithm offers a higher level of security but entails higher computing costs. There is a trade-off between symmetric and asymmetric algorithms: symmetric algorithms are better suited for time-sensitive applications, while RSA is essential for scenarios requiring heightened security, especially in vehicular networks where transaction integrity is critical [43].

- **Blockchain Solutions:** The implementation of blockchain protocols, such as the VChain protocol presented by Kumar et al. [44], demonstrates the benefits of decentralized security models that strengthen defenses against cyberattacks. These protocols outperform traditional methods by guaranteeing consistent performance, even under variable network conditions. The VChain protocol effectively tackles vulnerabilities such as replay attacks, which are essential for secure Vehicle-to-Infrastructure (V2I) communications [44].

- **Public Key Infrastructure and Crypto Agility:** The integration of Public Key Infrastructure (PKI) with the principles of cryptographic agility facilitates a flexible response to emerging security threats in intelligent transportation systems [45]. This approach enables cryptographic methods to be adapted to evolving vulnerabilities, thereby enhancing the overall security of these systems [46]. This flexibility is essential for dealing with the specific vulnerabilities present in vehicular networks and underlines the importance of continuous innovation in cryptographic strategies.

- **Emerging Cryptographic Concepts:** Research into cutting-edge cryptographic methods, including Elliptic Curve Cryptography (ECC) and post-quantum cryptography, offers valuable opportunities to enhance security while minimizing the impact on performance [47]. Elliptic curve cryptography, known for its efficiency and compact key size, is particularly relevant for smart city applications where computing resources may be limited [48].

In conclusion, traditional cryptographic algorithms offer fast processing capabilities, while blockchain-based solutions offer enhanced security and resilience against cyber threats, making them more advantageous for vehicular communication scenarios. Future research should prioritize comparative evaluations of the performance of these algorithms under different network conditions, and continue to explore innovative cryptographic techniques designed to meet the specific requirements of intelligent transport systems. This in-depth understanding will be essential to promote the adoption of blockchain technology in the protection of vehicular communication networks.

5.3 Security Measures in Connected Vehicle Security Blockchain Solution

The cryptographic algorithms ensure the secure encryption of the key exchange for communication purposes [31]. Each vehicle's unique signature is meticulously maintained within the model to promptly detect any fraudulent activities; even minor deviations in signatures trigger immediate alerts. Vehicles securely transmit traffic bytes within the model, including end-to-end encrypted message payloads readable solely by the intended recipient possessing the AES keys [49]. During message sharing via radar systems, vehicles sign their message packets, with signed radar frames subsequently transferred. The recipient can authenticate the sender and proceed with the decryption process [50]. All these message frames and radar shares are stored as blocks within the vehicle's blockchain network for future verification by law enforcement agencies [31].

In the context of connected vehicle technology, current security measures address the multitude of safety concerns surrounding automotive safety [51]. These measures safeguard all security protocols. Firstly, only authenticated users gain access to the connected vehicle network, with vehicle identity keys linked to digital private keys and public addresses recorded in the blockchain [52].

The integration of blockchain technology provides an essential security framework, enabling swift detection and mitigation of both known and zero-day external and internal threats without disrupting operations [53]. The immutability of the universal ledger ensures superior security levels crucial in the connected vehicle environment, where accidents can occur without time for system updates or antivirus sweeps. Additionally, the absence of centralized points of control alleviates the burden of managing heavy traffic flow, ensuring the network remains scalable as per its original design [54]. Within the Operational Environment Domains, this system acts as a barrier against cyber-terrorist activities, allowing data flow within the system to remain undetected.

Blockchain-based vehicle data marketplace model secures and efficiently shares connected car data, including black box video, while allowing data owners to control their data and access control lists [55]. Blockchain technology enhances connected vehicle security by providing comprehensive and end-to-end protection, ensuring trusted and secure vehicles [10]. Additionally, it ensures trusted communications and prevents falsified information in cooperative ramp merging applications, thereby securing connected vehicle security [56].

5.4 Integration with Automotive Supply Chain

Blockchain technology has attracted worldwide interest for its role in authenticating, securing, and optimizing business processes [57]. The Automotive industry is innovative in integrating blockchain technology into different business areas. The combination of the blockchain with the Internet of the vehicle V2V and V2X to secure communication for the benefit of road safety has become part of the academic research interest [58]. Blockchain technology has been suggested for revolutionizing the existing centralized-based identification frameworks to secure the communication among the vehicles and the entire vehicle network mentioned as, Secure and Intelligent Vehicle Network (SIVN) and later Extended SIVN (ESIVN) [59].

In many cases of the automotive supply chain, even a very hostile attacker may not be able to alter the bogus data, since the whole block before getting added to the blockchain, passes through a complex mechanism while getting verified by several thousands of nodes in the network [9]. Therefore, the final block would contain the true information related to the particular auto and that legitimacy can be verified through the smartphone application given. Moreover, if the data is legit, then the del dealer will pay the same amount of gas which will make sure the automotive supply chain entities may never alter the data [60].

Car manufacturers utilize the connected vehicle control unit as an IoT gateway for external communication [36]. Enhancing the security of connected vehicles solely through anti-hacking systems is challenging due to the numerous access points [61]. The blockchain serves as an immutable peer-to-peer ledger capable of recording product data within the vehicle supply chain. As participants in the automotive supply chain change rapidly under the circular economy paradigm, ensuring the credibility of Vehicle ID, cross-chain product data, and billing on the blockchain network is crucial [62]. Blockchain standards for Vehicle-to-X communication are evolving to improve data interoperability. However, some argue that blockchain primarily focuses on network security, trust, and governance management rather than enhancing data interoperability [63]. Agreement among participants on a standard and allocation of IT resources for development and operation is necessary.

Blockchain, as a decentralized technology, addresses the shortcomings of centralized database systems, including single points of failure, unauthorized data access, and insufficient privacy and security [64]. Consequently, blockchain emerges as a promising solution for optimizing the physical flow within automotive supply chains [65]. Many companies across industries have developed blockchain supply chain solutions based on permissioned blockchains (private blockchains) due to their superior security, privacy, and performance compared to public blockchains. Although permissioned blockchains offer security, only authorized nodes can access transaction data [66]. However, with the automotive supply chain's increasing complexity and the integration of external entities for Vehicle-to-X communication, the public may perceive a participant as a "trusted" company within the blockchain network, raising concerns regarding product security and integrity throughout the supply chain [67].

5.5 Enhancing Physical Flow in the Automotive Supply Chain

Supply chain physical flows have the same status as information and financial flows in logistics management. Nowadays, organizations seek for combined physical and informational flow to move around the resources (or products) from supplier to internal organization through a network of distribution and end users [68]. Automotive parts suppliers in the automotive industry at the different levels of the product structure send these parts assembled or disassembled to the assembly plant shop line either locally or worldwide. It is clear that the part message during the messaging process is to be trustworthy and secure, so the role of the suppliers is the most crucial one in the process [30]. Blockchain technology is designed to prove the traceability, authenticity, and integrity of various kinds of products in the supply chain. A highly secure blockchain-based solution streamlines cross-border automotive part movements by assigning digital compliance certificates to individuals, organizations, or countries using blockchain and smart contract technologies [69].

Blockchain, hailed as distributed ledger technology focused on security and confidentiality [30], ensures privacy by restricting access to authorized roles only. The real-time parts management system must embrace blockchain technology to establish a networked and transparent traceable system. The privacy-enhancing transport market discourages combining access control with data posting, a practice known as subjective access policy [70]. With the advent of the Internet of Vehicles (IoV), drones, vehicles, and roadside units can securely communicate and share interconnected transport data over the blockchain. Blockchain effectively manages all links between transport data and owner keys for specific nodes, preventing tampering with vehicle nodes executing behavioral tasks and allowing vehicles to participate in consensus methods for link-sharing agreements [35].

Blockchain technology has established itself as a leading solution for Internet of Vehicles (IoV) applications, providing a secure, scalable, transparent, and tamper-proof data-sharing platform among entities [35]. Introducing a novel blockchain infrastructure tailored for IoV systems ensures secure, anonymous transactions for embedded systems [71]. This infrastructure prioritizes lightweight and rapid verification, allowing the Industrial Internet of Vehicles (IIoV) to transform non-trust environments for resource exchange. Specifically, blockchain-based reputation mechanisms are implemented to maintain vehicle and parts reputation scores [71].

Furthermore, an innovative scheme has been devised to enable secure, real-time transmission in multi-hop vehicular networks [72]. This approach combines pay channel-based off-chain systems with an on-chain game theory-proof scheme to achieve low latency and time-coordinated systems within this network environment. A lightweight, end-to-end product traceability system for the Internet of Vehicles (IoV) can be achieved using an authorization-based blockchain [73]. This approach enhances transparency and security, enabling secure data exchange between authorized stakeholders while guaranteeing unforgeable information on the provenance and movement of products, thus promoting trust in the supply chain.

5.6 Challenges in Implementing Connected Vehicle Security Blockchain Solution

A fundamental aspect of automotive manufacturing is its collaborative nature, necessitating extensive data sharing between entities along the supply chain [62]. The significance of this data, encompassing specific vehicle details, emission values, and fuel consumption, crucial for calculating fleet or supply chain-level efficiencies, demands high quality and accuracy.

While data quality can be easily ensured, accuracy mandates validation through a verification mechanism or trust-based relationships. Centralized intermediaries can establish necessary trust relationships among parties, but pose risks of data breaches or modifications.

In contrast, blockchain, a decentralized solution, ensures data trust by combining decentralization and trustworthiness, leading to successful commercial applications [74]. This reduces intermediary costs for governmental authorities, primarily constituted by transaction costs, thereby encouraging technology adoption and contributing significantly to institutional economics.

However, transparency and privacy pose challenges, sparking disputes among consortium members seeking secure information sharing [62]. While crucial information must be shared, the need for privacy protection and data control complicates matters. Entities may find it unacceptable to disclose strategic information to other consortium members without hiding it from others.

The rapid expansion of the automotive industry has exposed it to various malicious activities, posing escalating security threats to vehicle identity, integrity, and resilience within its supply chain [75]. In the automotive manufacturing lifecycle, vehicles incorporate billions of parts, necessitating the transmission of logistics information among numerous stakeholders. Introducing digital technology to revolutionize these processes can mitigate cyber threats and ensure continuous validation of a secure supply chain. However, the vast volume of data poses the initial challenge: establishing an efficient and reliable data-sharing infrastructure among participants striving for comprehensive optimization.

To address these challenges, each car part, laden with vehicle data, contains thousands to millions of attributes, requiring the system to process an unprecedented volume of data points annually. Addressing these challenges mandates a solution centered on extensive decentralization and the absence of intermediary authorities [76].

5.7 Case Studies: Implementing Connected Vehicle Security Blockchain Solutions for Enhanced Automotive Supply Chain Flow

The manufacturing process starts with the creation of a permissioned blockchain, incorporating public input and API auxiliary validation. During the master control phase, various business aspects are unified using different smart contract templates and calls. Transactions are managed by organizing blocks in chronological order and creating hash digital proofs. Data preservation involves storing significant amounts of data and sharing accumulated information. Credit upload connects obtained credit with hash digital proofs and block numbers. Credit inquiries use timestamps to retrieve historical credit uploads. The parameter starting phase initializes user accounts for bidding and enables owners to participate in specific smart contracts, facilitating successful car starts and tests. Key storage combines user private/public keys and file encryption [77].

The focus is on using blockchain technology to enhance security and logistics in the automotive supply chain, particularly for connected vehicles. While much of the research remains theoretical, various studies have explored practical implementations [78]. For example, Xia et al. discussed a method for exchanging data between vehicles and entities, highlighting improved vehicle operations through shared event information [79]. Demir et al. proposed a tamper-free ledger for auto insurance records, improving the transaction experience and dispute resolution [80]. Patel et al. introduced the VehicleChain scheme, improving secure vehicle-to-vehicle and vehicle-to-infrastructure communications [81]. In addition, Abbade et al. presented a blockchain architecture for secure vehicle data recording, addressing key challenges such as odometer fraud [82].

Notable examples include the Vehicular network Based Consensus Algorithm (VBCA) and Full Duplex Non-Orthogonal Multiple Access (FD-NOMA), which have shown potential for improving data security and operational efficiency [83]. Theoretical evaluations of these technologies suggest improvements in transaction throughput and latency [84]. However, the experimental designs used in these studies vary, and specific details concerning the scale and duration of experiments are often lacking. This highlights the need for further research into practical implementation, including controlled trials that assess the effectiveness of these solutions under real-life conditions. Such future studies could provide valuable insights into the opportunities and challenges offered by blockchain technology, particularly for the automotive supply chain.

The Table 1 below summarizes various articles focusing on the integration of blockchain technology into vehicle networks and automotive supply chains. Each article contributes to enhancing security, efficiency, or trust in these systems using different methods and algorithms. However, they also acknowledge limitations such as integration challenges, resource-intensive algorithms, and privacy concerns. The methods employed include blockchain frameworks, consensus algorithms, cryptographic protocols, and distributed frameworks.

Table 1: Enhancing security in vehicular networks: A review of blockchain solutions

Article references	Contributions	Limitations	Methods used
[85]	VBCA algorithm proposal for data security in vehicular networks	Integration challenges due to time-sensitive message broadcasting; resource-intensive PoW algorithm	Vehicular network Based Consensus Algorithm (VBCA); consortium blockchain
[86]	A multi-level blockchain framework enhances security and efficiency in IoV	–	Multi-level blockchain framework; ECDSA and ECDH key agreement
[87]	Enhanced goodput and security in the vehicular network using FD-NOMA	Increasing complexity of connected nodes and rising threats	Full Duplex Non-Orthogonal Multiple Access (FD-NOMA)
[88]	Secure V2V communication using blockchain and smart contracts	–	Smart contracts, blockchain
[89]	Improved trustworthiness and security in data sharing for IoV	Trust issues and privacy concerns in IoV	Modified-Two-stage Auction Algorithm (M-ITA); Discrete Particle Swarm Optimization (DPSO)
[90]	Enhances privacy and security in connected vehicles using zk-SNARK protocol	Single point of failure in centralized trusted bodies	zk-SNARK protocol over blockchain
[62]	Enhances security and transparency in the automotive supply chain using Hyperledger Fabric	Centralized database access can lead to record tampering	Permissioned blockchain; Hyperledger Fabric
[91]	Preserves users' privacy while boosting vehicle security	–	Blockchain-based methodology
[92]	Enhances security and trust computation in IoV	–	Blockchain; trust computation
[93]	Enhances smart vehicle security using blockchain	–	Blockchain-based architectural framework

6 Discussion

In recent years, vehicular communication has become increasingly critical for enhancing road safety and driving efficiency. Traditional vehicle-key authentication systems, however, are vulnerable to various attacks, jeopardizing system security. The automotive sector faces significant risks from Sybil, DoS, and Eclipse attacks within the Internet of Vehicles (IoV). These threats highlight the necessity for robust security mechanisms in connected vehicle systems.

Blockchain technology, renowned for providing secure, transparent, and decentralized transactions, offers a promising solution to these security challenges. By validating transactions using cryptographic techniques and securely storing them in blocks, blockchain can enhance security across various sectors, including transportation. In the automotive industry, blockchain-based solutions address the challenges posed by third-party intermediaries, offering a more secure and efficient method for managing transactions and processing data. While blockchain technology presents transformative potential, its high computing costs and latency remain challenges.

The results highlight how blockchain reduces unauthorized access to vehicles and improves data integrity in real-time communication. Additionally, blockchain's real-time data-sharing capabilities enhance decision-making processes between stakeholders, a crucial factor as the automotive industry moves toward greater interconnectivity.

This chapter presents an in-depth look at the application of blockchain in the automotive sector, focusing on connected vehicle security and supply chain integration. The results demonstrate that blockchain reduces instances of unauthorized access and enhances data integrity in real-time vehicle communications. Blockchain's role in improving real-time data sharing also promotes more efficient decision-making processes, which is vital as interconnected systems increasingly rely on timely information to optimize operations.

Fig. 5 illustrates blockchain's integration into connected vehicles, showing key components that bolster security and operational efficiency. It begins with data collection from vehicles, followed by vehicle authentication to prevent unauthorized access. Transactions are validated with cryptographic techniques and stored in a decentralized blockchain network, enabling secure, real-time communication between vehicles and stakeholders. Artificial Intelligence (AI) further enhances these capabilities through anomaly detection and advanced encryption.

Furthermore, the study demonstrates blockchain's potential to reduce cybersecurity risks in vehicle ecosystems. In addition to blockchain, AI integration promises to advance security with adaptive encryption and AI-driven anomaly detection, enabling AI's role in designing quantum-resistant cryptographic protocols to safeguard against emerging threats. Combining AI and blockchain, therefore, offers significant improvements in security and operational efficiency for automotive systems.

In traditional automotive supply chains, incompatible databases create inefficiencies. Blockchain technology offers a solution that guarantees data integrity, high availability, security, and trust among parties. Blockchain applications in connected vehicles go beyond authentication and data sharing to include component traceability and warranty management. By recording transactions in real time, blockchain improves operational efficiency, accountability, and safety in the supply chain, enhancing customer satisfaction.

To maximize the benefits of blockchain, it is recommended to integrate it with authorizations for owner identity certification in commerce and insurance, to use real-name systems for driver and vehicle tracking, and to combine blockchain with IoT for secure data validation and fair insurance practices.

Despite the transformative potential of blockchain technology, high IT costs and latency represent significant challenges for resource-constrained industries such as automotive. These issues can lead to delays in real-time decision-making, which is essential in connected vehicle applications. To address these challenges, current research focuses on more efficient consensus mechanisms, such as proof-of-stake or delegated proof-of-stake, as well as off-chain solutions that enable faster transaction processing without compromising security.

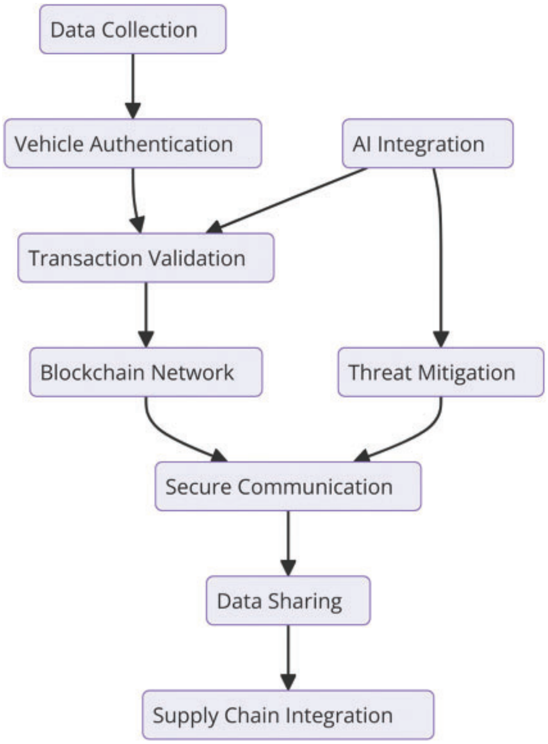

Figure 5: Blockchain integration process in connected vehicle networks

Another significant challenge is **scalability**, as vehicle and transaction volume increase strains existing blockchain frameworks. Research should focus on **scalable blockchain frameworks** that meet the growing demands of the automotive industry.

Regulatory hurdles must also be overcome to facilitate widespread adoption. The study highlights the importance of developing legal frameworks that can support the integration of blockchain into automotive applications to address potential liability and privacy concerns. By addressing these limitations, researchers can provide a more balanced view of the impact of blockchain technology on the automotive industry.

While integrating blockchain into connected vehicles has great potential, regulatory challenges remain a significant obstacle. Nevertheless, the use of public key cryptography combined with decentralized blockchain technology offers a promising solution for enhancing network security within vehicle ecosystems. This approach strengthens the integrity and security of interactions, including vehicle-to-vehicle, vehicle-to-infrastructure, and vehicle-to-cloud communications. By guaranteeing secure, reliable data exchange and protecting against key violations, blockchain enables seamless, reliable communication between vehicles and the wider network.

Fig. 6 illustrates the integration of blockchain into vehicle networks, describing the interactions between vehicles, the blockchain network, security services, manufacturers, and supply chain systems. These entities collectively manage transactions and guarantee system integrity through validation and real-time updates.

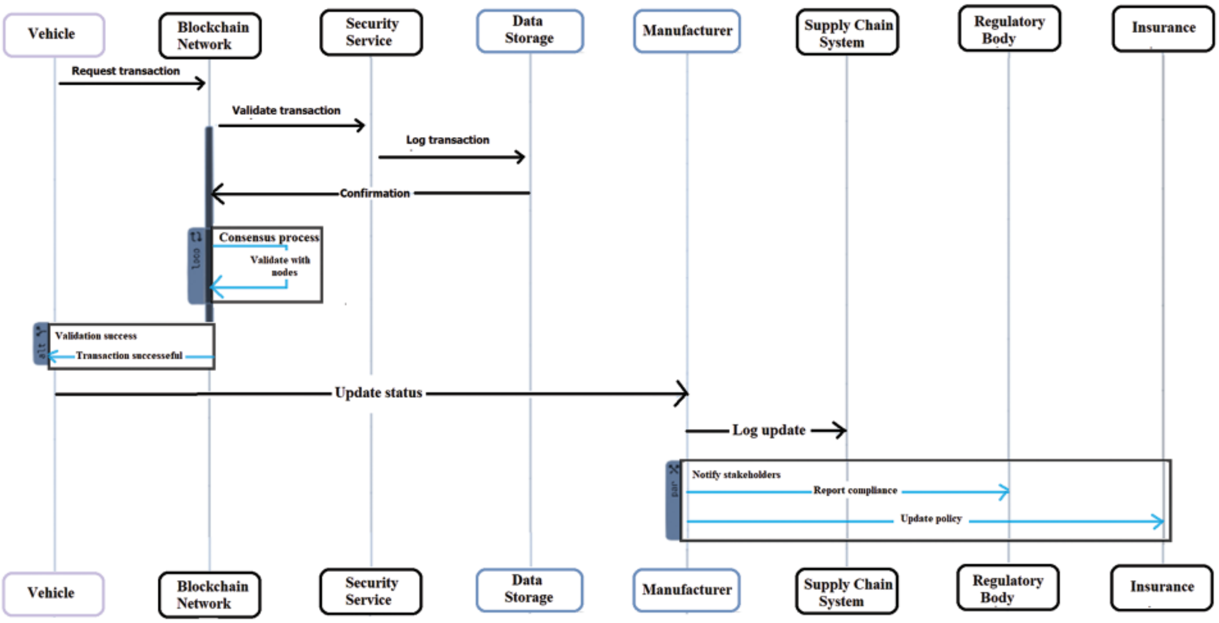

Figure 6: Integrating blockchain in connected vehicle networks: interactions and system integrity

Future Research Directions:

- **Technical Solutions:** Identifying strategies to overcome scalability and interoperability issues in blockchain implementations within the automotive industry.
- **Regulatory Frameworks:** Investigating the development of legal frameworks that could facilitate the safe and effective use of blockchain in automotive applications.
- **Integration with Emerging Technologies:** Exploring the synergistic effects of combining blockchain with IoT and AI, and how these integrations can enhance overall vehicle security and performance.

By addressing these areas, researchers and business practitioners can contribute to a more seamless transition to blockchain solutions within the automotive industry, ultimately enhancing the security of connected vehicles and the efficiency of the supply chain.

7 Conclusion

Blockchain technology offers effective solutions to security gaps in connected vehicle systems and automotive supply chains. Conventional authentication methods are often insufficient in the face of advanced cyber threats, while blockchain's decentralized structure facilitates secure transactions and reliable communication between vehicles and supply chain participants. The integration of AI enhances these solutions by refining cryptographic techniques, automating key management processes, and identifying anomalies.

To effectively implement these blockchain solutions, car manufacturers and supply chain managers should launch pilot programs focusing on areas such as component traceability and warranty management. Collaboration with technology partners can facilitate the development of tailored solutions. In addition, clear regulatory frameworks are essential to promote safe adoption.

Future studies should concentrate on scalable blockchain architectures and investigate the synergistic interactions between blockchain, IoT, and AI, thereby enhancing the safety and efficiency of connected vehicles and automotive supply chains.

Acknowledgement: Not applicable.

Finding Statement: The authors declare that no funding was received for this study.

Author Contributions: The authors confirm contribution to the paper as follows: study conception and design: Khadija El Fellah and Ikram El Azami; data collection: Khadija El Fellah; analysis and interpretation of results: Khadija El Fellah, Ikram El Azami, and Adil El Makrani; draft manuscript preparation: Khadija El Fellah and Ikram El Azami; review and editing: Ikram El Azami, Habiba BOUIJIJ, and Oussama El Azzouzy; visualization: Khadija El Fellah, Ikram El Azami, and Adil El Makrani; supervision: Ikram El Azami and Adil El Makrani; project administration: Ikram El Azami and Adil El Makrani; contributions and assistance: Habiba Bouijij and Oussama El Azzouzy; funding acquisition: Khadija El Fellah. All authors reviewed the results and approved the final version of the manuscript.

Availability of Data and Materials: Data sharing is not applicable to this article as no datasets were generated or analyzed during the current study.

Ethics Approval: The authors declare that ethical approval was not required for this study.

Conflicts of Interest: The authors declare no conflicts of interest to report regarding the present study.

References

[1] T. Alladi, V. Chamola, N. Sahu, V. Venkatesh, A. Goyal and M. Guizani, “A comprehensive survey on the applications of blockchain for securing vehicular networks,” *IEEE Commun. Surv. Tut.*, vol. 24, no. 2, pp. 1212–1239, 2022. doi: 10.1109/COMST.2022.3160925.

[2] C. Schleiffer, M. Wolf, A. Weimerskirch, and L. Wolleschensky, “Secure key management–A key feature for modern vehicle electronics,” in *SAE Technical Paper 2013-01-1418*. doi: 10.4271/2013-01-1418.

[3] M. Platt and P. McBurney, “Sybil in the Haystack: A comprehensive review of blockchain consensus mechanisms in search of strong sybil attack resistance,” *Algorithms*, vol. 16, no. 1, Jan. 2023, Art. no. 34. doi: 10.3390/a16010034.

[4] K. Dwivedi, A. Agrawal, A. Bhatia, and K. Tiwari, “A novel classification of attacks on blockchain layers: Vulnerabilities, attacks, mitigations, and research directions,” 2024. doi: 10.48550/ARXIV.2404.18090.

[5] R. Uddin, S. A. P. Kumar, and V. Chamola, “Denial of service attacks in edge computing layers: Taxonomy, vulnerabilities, threats and solutions,” *Ad Hoc Netw.*, vol. 152, no. 11, Jan. 2024, Art. no. 103322. doi: 10.1016/j.adhoc.2023.103322.

[6] S. Alshathri, A. Sayed, and E. E. -D. Hemdan, “An intelligent attack detection framework for the internet of autonomous vehicles with imbalanced car hacking data,” *World Elect. Veh. J.*, vol. 15, no. 8, Aug. 2024, Art. no. 8. doi: 10.3390/wevj15080356.

[7] D. X. Wang, “Federated learning approaches for collaborative threat detection in autonomous vehicle networks,” *J. Artif. Intell. Res. Appl.*, vol. 4, no. 1, Jun. 2024, Art. no. 1.

[8] N. Kshetri, I. Sultana, M. M. Rahman, and D. Shah, “DefTesPY: Cyber defense model with enhanced data modeling and analysis for Tesla company via Python Language,” 19 Jul. 2024. doi: 10.48550/arXiv.2407.14671.

[9] T. Rathod *et al.*, “Blockchain-driven intelligent scheme for IoT-based public safety system beyond 5G networks,” *Sensors*, vol. 23, no. 2, Jan. 2023, Art. no. 969. doi: 10.3390/s23020969.

[10] Y. Balasubramaniam, and S. PSV, “Enhancing connected vehicle security with block chain,” *Int. J. Adv. Sci. Res. Eng.*, vol. 4, no. 8, pp. 189–193, 2018. doi: 10.31695/ijasre.2018.32849.

[11] K. E. Fellah, I. E. Azami, and A. E. Makrani, “A comparative analysis of blockchain and Electronic Data Interchange (EDI) in supply chain: Identifying strengths, weaknesses, and synergies,” *J. Autonom. Intell.*, vol. 7, no. 5, 2024, Art. no. 1481. doi: 10.32629/jai.v7i5.1481.

[12] M. Alsadi, J. Arshad, J. Ali, A. Prince, and S. Shishank, “TruCert: Blockchain-based trustworthy product certification within autonomous automotive supply chains,” *Comput. Elect. Eng.*, vol. 109, no. 2, Aug. 2023, Art. no. 108738. doi: 10.1016/j.compeleceng.2023.108738.

[13] N. Tabassum and C. R. K. Reddyy, “Review on QoS and security challenges associated with the internet of vehicles in cloud computing,” *Meas. Sens.*, vol. 27, no. 3, Jun. 2023, Art. no. 100562. doi: 10.1016/j.measen.2022.100562.

[14] A. Vaghani, K. Sood, and S. Yu, “Security and QoS issues in blockchain enabled next-generation smart logistic networks: A tutorial,” *Blockchain: Res. Appl.*, vol. 3, no. 3, Sep. 2022, Art. no. 100082. doi: 10.1016/j.bcra.2022.100082.

[15] N. S. Mohammed, O. A. Dawood, A. M. Sagheer, and A. A. Nafea, “Secure smart contract based on blockchain to prevent the non-repudiation phenomenon,” *Baghdad Sci. J.*, May 2023. doi: 10.21123/bsj.2023.8164.

[16] M. Karl, M. Musch, G. Ma, M. Johns, and S. Lekies, “No keys to the kingdom required: A comprehensive investigation of missing authentication vulnerabilities in the wild,” in *Proc. 22nd ACM Internet Measurem. Conf., IMC ’22*, New York, NY, USA, Association for Computing Machinery, Oct. 2022, pp. 619–632. doi: 10.1145/3517745.3561446.

[17] A. Nash, H. Studiawan, G. Grispos, and K. -K. R. Choo, “Security analysis of google authenticator, microsoft authenticator, and authy,” in *Digital Forensics and Cyber Crime*, S. Goel, P. R. Nunes de Souza, Eds., Cham: Springer Nature Switzerland, 2024, pp. 197–206. doi: 10.1007/978-3-031-56583-0_13.

[18] Z. Lamoyero and O. Fajana, “Exposed: Critical vulnerabilities in USSD banking authentication protocols,” in *IEEE Int. Conf. Cyber Secur. Resil. (CSR)*, Jul. 2023, pp. 275–280. doi: 10.1109/CSR57506.2023.10224933.

[19] M. Castillo, G. Voce, H. Griffith, and H. Rathore, “Poster: Decentralized simulation workflow for enhancing connected vehicle security,” in *Proc. Twenty-fourth Int. Symp. Theory, Algor. Found. Protocol Des. Mob. Netw. Mob. Comput. MobiHoc ’23*, New York, NY, USA, Association for Computing Machinery, Oct. 2023, pp. 574–576. doi: 10.1145/3565287.3617981.

[20] S. Yadav, K. Singh, and S. Bezzateev, “Enhancing security using trusted blockchain method for internet of vehicle,” in *2024 Int. Conf. Automat. Comput. (AUTOCOM)*, Mar. 2024, pp. 512–518. doi: 10.1109/AUTOCOM60220.2024.10486132.

[21] M. Azath and V. Singh, “An approach to preventing vehicular ad-hoc networks from malicious nodes based on blockchain,” *Rev. Comput. Eng. Res.*, vol. 10, no. 1, pp. 16–27, 2023. doi: 10.18488/76.v10i1.3324.

[22] Y. V. R. S. Viswanadham and K. Jayavel, “A framework for data privacy preserving in supply chain management using hybrid meta-heuristic algorithm with ethereum blockchain technology,” *Electronics*, vol. 12, no. 6, Jan. 2023, Art. no. 6. doi: 10.3390/electronics12061404.

[23] A. Ghosh, S. Gupta, A. Dua, and N. Kumar, “Security of cryptocurrencies in blockchain technology: State-of-art, challenges and future prospects,” *J. Netw. Comput. Appl.*, vol. 163, no. 1, Aug. 2020, Art. no. 102635. doi: 10.1016/j.jnca.2020.102635.

[24] K. El Fellah, A. El Makrani, and I. El Azami, “The impact of blockchain technology and business intelligence on the supply chain performance-based tracking process,” in *Digital Technologies and Applications*, S. Motahhir, B. Bossoufi, Eds., Cham: Springer Nature Switzerland, 2023, pp. 845–854. doi: 10.1007/978-3-031-29857-8_84.

[25] B. Shrimali and H. B. Patel, “Blockchain state-of-the-art: Architecture, use cases, consensus, challenges and opportunities,” *J. King Saud Univ. Comput. Inf. Sci.*, vol. 34, no. 9, pp. 6793–6807, Oct. 2022. doi: 10.1016/j.jksuci.2021.08.005.

[26] K. El Fellah, A. El Makrani, and I. El Azami, “Improving the application of blockchain technology for tracking processes in the supply chain integrated business intelligence,” in *Modern Artificial Intelligence and Data Science: Tools, Techniques and Systems*, A. Idrissi, Ed., Cham: Springer Nature Switzerland, 2023, pp. 201–211. doi: 10.1007/978-3-031-33309-5_16.

[27] F. Bassan and M. Rabitti, “From smart legal contracts to contracts on blockchain: An empirical investigation,” *Comput. Law Secur. Rev.*, vol. 55, Nov. 2024, Art. no. 106035. doi: 10.1016/j.clsr.2024.106035.

[28] S. EL Madani, S. Motahhir, and A. EL Ghzizal, “Internet of vehicles: Concept, process, security aspects and solutions,” *Multimed. Tools Appl.*, vol. 81, no. 12, pp. 16563–16587, May 2022. doi: 10.1007/s11042-022-12386-1.

[29] U. Arshad, Z. Halim, H. Alasmary, and M. Waqas, “Futuristic decentralized vehicular network architecture and repairing management system on blockchain,” *IEEE Internet Things J.*, vol. 11, no. 13, pp. 23604–23616, Jul. 2024. doi: 10.1109/JIOT.2024.3386600.

[30] C. -L. Chen, Z. -P. Zhu, M. Zhou, W. -J. Tsaur, C. -M. Wu and H. Sun, “A secure and traceable vehicles and parts system based on blockchain and smart contract,” *Sensors*, vol. 22, no. 18, Sep. 2022, Art. no. 6754. doi: 10.3390/s22186754.

[31] G. Rathee, A. Sharma, R. Iqbal, M. Aloqaily, N. Jaglan and R. Kumar, “A blockchain framework for securing connected and autonomous vehicles,” *Sensors*, vol. 19, no. 14, 2019, Art. no. 3165. doi: 10.3390/s19143165.

[32] P. Gaba, R. S. Raw, O. Kaiwartya, and M. Aljaidi, “B-SAFE: Blockchain-enabled security architecture for connected vehicle fog environment,” *Sensors*, vol. 24, no. 5, Jan. 2024, Art. no. 5. doi: 10.3390/s24051515.

[33] S. Hussain, S. Tahir, A. Masood, and H. Tahir, “Blockchain-enabled secure communication framework for enhancing trust and access control in the internet of vehicles (IoV),” *IEEE Access*, vol. 12, pp. 110992–111006, 2024. doi: 10.1109/ACCESS.2024.3431279.

[34] G. Habib, S. Sharma, S. Ibrahim, I. Ahmad, S. Qureshi and M. Ishfaq, “Blockchain technology: Benefits, challenges, applications, and integration of blockchain technology with cloud computing,” *Fut. Intern.*, vol. 14, no. 11, 2022, Art. no. 11. doi: 10.3390/fi14110341.

[35] M. B. Mollah *et al.*, “Blockchain for the internet of vehicles towards intelligent transportation systems: A survey,” *IEEE Internet Things J.*, vol. 8, no. 6, pp. 4157–4185, Mar. 2021. doi: 10.1109/JIOT.2020.3028368.

[36] V. Dedeoglu *et al.*, “A journey in applying blockchain for cyberphysical systems,” in *Int. Conf. Commun. Syst. Netw. (COMSNETS)*, Jan. 2020, pp. 383–390. doi: 10.1109/COMSNETS48256.2020.9027487.

[37] F. Azam, A. Biradar, N. Priyadarshi, S. Kumari, and S. Tangade, “A review of blockchain based approach for secured communication in internet of vehicle (IoV) scenario,” in *Second Int. Conf. Smart Technol. Comput., Elect. Electr. (ICSTCEE)*, Dec. 2021, pp. 1–6. doi: 10.1109/ICSTCEE54422.2021.9708555.

[38] P. Dutta, T-M. Choi, S. Somani, and R. Butala, “Blockchain technology in supply chain operations: Applications, challenges and research opportunities,” *Transport. Res. Part E: Logist. Transport. Rev.*, vol. 142, no. 3, Oct. 2020, Art. no. 102067. doi: 10.1016/j.tre.2020.102067.

[39] P. Surapaneni, S. Bojjagani, V. C. Bharathi, M. Kumar Morampudi, A. Kumar Maurya and M. Khurram Khan, “A systematic review on blockchain-enabled internet of vehicles (BIoV): Challenges, defenses, and future research directions,” *IEEE Access*, vol. 12, no. 1, pp. 123529–123560, 2024. doi: 10.1109/ACCESS.2024.3453433.

[40] Y. Li, K. Ouyang, N. Li, R. Rahmani, H. Yang and Y. Pei, “A Blockchain-assisted intelligent transportation system promoting data services with privacy protection,” *Sensors*, vol. 20, no. 9, Jan. 2020, Art. no. 9. doi: 10.3390/s20092483.

[41] C. Silva, V. A. Cunha, P. Barraca Jão, and R. L. Aguiar, “Analysis of the cryptographic algorithms in IoT communications,” *Inf. Syst. Front.*, vol. 26, no. 4, pp. 1243–1260, Aug. 2024. doi: 10.1007/s10796-023-10383-9.

[42] M. Alenezi, H. Alabdulrazzaq, and N. Mohammad, “Symmetric encryption algorithms: Review and evaluation study,” *Int. J. Commun. Netw. Inform. Secur.*, vol. 12, Aug. 2020, Art. no. 256.

[43] M. A. Shawky *et al.*, “How secure are our roads? An in-depth review of authentication in vehicular communications,” *Veh. Commun.*, vol. 47, no. 2, Jun. 2024, Art. no. 100784. doi: 10.1016/j.vehcom.2024.100784.

[44] A. Kumar, A. S. Yadav, and D. S. Kushwaha, "VChain: Efficient blockchain based vehicular communication protocol," in *10th Int. Conf. Cloud Comput. Data Sci. Eng. (Confluence)*, Jan. 2020, pp. 762–768. doi: 10.1109/Confluence47617.2020.9057801.

[45] A. Lamssaggad, N. Benamar, A. S. Hafid, M. Msahli, "A survey on the current security landscape of intelligent transportation systems," *IEEE Access*, vol. 9, pp. 9180–9208, 2021. doi: 10.1109/ACCESS.2021.3050038.

[46] S. E. Yunakovsky *et al.*, "Towards security recommendations for public-key infrastructures for production environments in the post-quantum era," *EPJ Quantum Technol.*, vol. 8, no. 1, Dec. 2021, Art. no. 1. doi: 10.1140/epjqt/s40507-021-00104-z.

[47] H. Gharavi, J. Granjal, and E. Monteiro, "Post-quantum blockchain security for the internet of things: Survey and research directions," *IEEE Commun. Surv. Tutorials*, vol. 26, no. 3, pp. 1748–1774, 2024. doi: 10.1109/COMST.2024.3355222.

[48] S. Ullah, J. Zheng, N. Din, M. T. Hussain, F. Ullah and M. Yousaf, "Elliptic curve cryptography; applications, challenges, recent advances, and future trends: A comprehensive survey," *Comput. Sci. Rev.*, vol. 47, no. 2, Feb. 2023, Art. no. 100530. doi: 10.1016/j.cosrev.2022.100530.

[49] M. D. Pese, "Bringing practical security to vehicles," Thesis, Univ. of Michigan, USA, 2022. doi: 10.7302/5977.

[50] M. C. Chow, M. Ma, and Z. Pan, "Attack models and countermeasures for autonomous vehicles," in *Intelligent Technologies for Internet of Vehicles*, N. Magaia, G. Mastorakis, C. Mavromoustakis, E. Pallis, E. K. Markakis, Eds., Cham: Springer International Publishing, 2021, pp. 375–401. doi: 10.1007/978-3-030-76493-7_12.

[51] A. Giannaros *et al.*, "Autonomous vehicles: Sophisticated attacks, safety issues, challenges, open topics, blockchain, and future directions," *J. Cybersecur. Priv.*, vol. 3, no. 3, Sep. 2023, Art. no. 3. doi: 10.3390/jcp3030025.

[52] G. Abdelkader, K. Elgazzar, and A. Khamis, "Connected vehicles: Technology review, state of the art, challenges and opportunities," *Sensors*, vol. 21, no. 22, Jan. 2021, Art. no. 22. doi: 10.3390/s21227712.

[53] Taskeen and S. Garai, "Emerging trends in cybersecurity: A holistic view on current threats, assessing solutions, and pioneering new frontiers," *Blockch. Heal. Tod.*, vol. 7, no. 1, Apr. 2024, Art. no. 302. doi: 10.30953/bhty.v7.302.

[54] T. R. Gadekallu *et al.*, "Blockchain for edge of things: Applications, opportunities, and challenges," *IEEE Internet Things J.*, vol. 9, no. 2, pp. 964–988, Jan. 2022. doi: 10.1109/JIOT.2021.3119639.

[55] A. Mohammad, S. Vargas, and P. Čermák, "Using blockchain for data collection in the automotive industry sector: A literature review," *J. Cybersecur. Priv.*, vol. 2, no. 2, Jun. 2022, Art. no. 2. doi: 10.3390/jcp2020014.

[56] A. Abdo, G. Wu, and N. Abu-Ghazaleh, "Secure ramp merging using blockchain," in *2021 IEEE Intell. Vehicles Symp. (IV)*, 2021, pp. 401–408. doi: 10.1109/iv48863.2021.9575411.

[57] P. Fraga-Lamas and T. M. Fernandez-Carames, "A review on blockchain technologies for an advanced and cyber-resilient automotive industry," *IEEE Access*, vol. 7, pp. 17578–17598, 2019. doi: 10.1109/ACCESS.2019.2895302.

[58] T. Huang *et al.*, "V2X cooperative perception for autonomous driving: Recent advances and challenges," 9 May 2024. doi: 10.48550/arXiv.2310.03525.

[59] Y. Wu, H-N. Dai, H. Wang, Z. Xiong, and S. Guo, "A survey of intelligent network slicing management for industrial IoT: Integrated approaches for smart transportation, smart energy, and smart factory," *IEEE Commun. Surv. Tut.*, vol. 24, no. 2, pp. 1175–1211, 2022. doi: 10.1109/COMST.2022.3158270.

[60] C. Kargacier, "Benefit and cost analysis of blockchain technology in the supply chain and monitoring in the automotive industry". Laurea, Politecnico di Torino, 2021. Accessed: Nov. 17, 2024. [Online]. Available: https://webthesis.biblio.polito.it/17716/.

[61] C. Vitale *et al.*, "CARAMEL: Results on a secure architecture for connected and autonomous vehicles detecting GPS spoofing attacks," *J. Wireless Com. Network*, vol. 2021, no. 1, 2021, Art. no. 115. doi: 10.1186/s13638-021-01971-x.

[62] S. Zafar, S. F. U. Hassan, A. S. Mohammad, A. A. Al-Ahmadi, and N. Ullah, "Implementation of a distributed framework for permissioned blockchain-based secure automotive supply chain management," *Sensors*, vol. 22, no. 19, Sep. 2022, Art. no. 7367. doi: 10.3390/s22197367.

[63] V. Malik *et al.*, "Building a secure platform for digital governance interoperability and data exchange using blockchain and deep learning-based frameworks," *IEEE Access*, vol. 11, pp. 70110–70131, 2023. doi: 10.1109/ACCESS.2023.3293529.

[64] A. Lowy, Z. Li, J. Liu, T. Koike-Akino, K. Parsons and Y. Wang, "Why does differential privacy with large epsilon defend against practical membership inference attacks," 14 Feb. 2024. doi: 10.48550/arXiv.2402.09540.

[65] G. Perboli, S. Musso, and M. Rosano, "Blockchain in logistics and supply chain: A lean approach for designing real-world use cases," *IEEE Access*, vol. 6, pp. 62018–62028, 2018. doi: 10.1109/ACCESS.2018.2875782.

[66] J. Al-Jaroodi and N. Mohamed, "Blockchain in industries: A survey," *IEEE Access*, vol. 7, pp. 36500–36515, 2019. doi: 10.1109/ACCESS.2019.2903554.

[67] R. Jabbar, M. Kharbeche, K. Al-Khalifa, M. Krichen, and K. Barkaoui, "Blockchain for the Internet of Vehicles: A decentralized IoT solution for vehicles communication using ethereum," *Sensors*, vol. 20, no. 14, Jan. 2020, Art. no. 14. doi: 10.3390/s20143928.

[68] A. Rahamneh, S. Alrawashdeh, A. Bawaneh, Z. Alatyat, A. Mohammad and S. Al-Hawary, "The effect of digital supply chain on lean manufacturing: A structural equation modelling approach," *Uncert. Supp. Chain Manag.*, vol. 11, no. 1, pp. 391–402, 2023.

[69] S. Dewangan, S. K. Verma, B. Parganiha, and S. Dewangan, "Applications and implementations of blockchain technology across the various sectors," in *Building Secure Business Models Through Blockchain Technology: Tactics, Methods, Limitations, and Performance*. IGI Global, pp. 1–19, 2023.

[70] J. Sychowiec and Z. Zieliński, "An experimental framework for secure and reliable data streams distribution in federated IoT environments," in *18th Conf. Comput. Sci. Intell. Syst. (FedCSIS)*, Sep. 2023, pp. 769–780. doi: 10.15439/2023F3882.

[71] Y. Wang, Y. Tian, X. Hei, L. Zhu, and W. Ji, "A novel IoV block-streaming service awareness and trusted verification scheme in 6G," *IEEE Trans. Vehicular Technol.*, vol. 70, no. 6, pp. 5197–5210, Jun. 2021. doi: 10.1109/TVT.2021.3063783.

[72] M. H. Z. Abidin, S. Suchaad, O. C. Yee, N. Ismail, and M. A. Abu, "Scalable off-chain blockchain for vehicular network," in *1st Int. Conf. Inform. Syst. Inform. Technol. (ICISIT)*, Jul. 2022, pp. 397–402. doi: 10.1109/ICISIT54091.2022.9873098.

[73] D. Stefanescu, L. Montalvillo, P. Galan-Garcia, J. Unzilla, and A. Urbieta, "A systematic literature review of lightweight blockchain for IoT," *IEEE Access*, vol. 10, pp. 123138–123159, 2022. doi: 10.1109/ACCESS.2022.3224222.

[74] Q-U-A. Arshad, W. Z. Khan, F. Azam, M. K. Khan, H. Yu and Y. B. Zikria, "Blockchain-based decentralized trust management in IoT: Systems, requirements and challenges," *Complex Intell. Syst.*, vol. 9, no. 6, pp. 6155–6176, Dec. 2023. doi: 10.1007/s40747-023-01058-8.

[75] A. O. Okomanyi, A. R. Sherwood, and E. Shittu, "Exploring effective strategies against cyberattacks: The case of the automotive industry," *Environ. Syst. Decis.*, vol. 44, no. 4, pp. 779–809, Dec. 2024. doi: 10.1007/s10669-024-09971-0.

[76] M. D. S. Ferdous, M. J. M. Chowdhury, K. Biswas, N. Chowdhury, and V. Muthukkumarasamy, "Immutable autobiography of smart cars leveraging blockchain technology," *Knowl. Eng. Rev.*, vol. 35, Jan. 2020, Art. no. e3. doi: 10.1017/S0269888920000028.

[77] I. M. Varma and N. Kumar, "A comprehensive survey on SDN and blockchain-based secure vehicular networks," *Veh. Commun.*, vol. 44, no. 4, Dec. 2023, Art. no. 100663. doi: 10.1016/j.vehcom.2023.100663.

[78] X. Xu, L. Tatge, X. Xu, and Y. Liu, "Blockchain applications in the supply chain management in German automotive industry," *Product. Plann. Cont.*, vol. 35, no. 9, pp. 917–931, Jul. 2024. doi: 10.1080/09537287.2022.2044073.

[79] Z. Xia, J. Wu, L. Wu, Y. Chen, J. Yang and P. S. Yu, “A comprehensive survey of the key technologies and challenges surrounding vehicular Ad Hoc networks,” *ACM Trans. Intell. Syst. Technol.*, vol. 12, no. 4, pp. 1–30, Jun. 2021. doi: 10.1145/3451984.

[80] M. Demir, O. Turetken, and A. Ferworn, “Blockchain based transparent vehicle insurance management,” in *2019 Sixth Int. Conf. Softw. Defined Syst. (SDS)*, Jun. 2019, pp. 213–220. doi: 10.1109/SDS.2019.8768669.

[81] A. Patel, N. Shah, T. Limbasiya, and D. Das, “VehicleChain: Blockchain-based vehicular data transmission scheme for smart city,” in *IEEE Int. Conf. Syst., Man Cyber. (SMC)*, 2019, pp. 661–667. doi: 10.1109/SMC.2019.8914391.

[82] L. R. Abbade *et al.*, “Blockchain applied to vehicular odometers,” *IEEE Netw.*, vol. 34, no. 1, pp. 62–68, Jan. 2020. doi: 10.1109/MNET.001.1900162.

[83] Y. Wang, H. Peng, Z. Su, T. H. Luan, A. Benslimane and Y. Wu, “A platform-free proof of federated learning consensus mechanism for sustainable blockchains,” *IEEE J. Sel. Areas Commun.*, vol. 40, no. 12, pp. 3305–3324, Dec. 2022. doi: 10.1109/JSAC.2022.3213347.

[84] M. T. Rana, M. Numan, M. Yousif, T. Hussain, A. Z. Khan and X. Zhao, “Enhancing sustainability in electric mobility: Exploring blockchain applications for secure EV charging and energy management,” *Comput. Elect. Eng.*, vol. 119, no. 3, Oct. 2024, Art. no. 109503. doi: 10.1016/j.compeleceng.2024.109503.

[85] N. U. Sehar *et al.*, “Blockchain enabled data security in vehicular networks,” *Sci. Rep.*, vol. 13, no. 1, Mar. 2023, Art. no. 4412. doi: 10.1038/s41598-023-31442-w.

[86] H. Lin, “Secure data transfer based on a multi-level blockchain for internet of vehicles,” *Sensors*, vol. 23, no. 5, Feb. 2023, Art. no. 2644. doi: 10.3390/s23052664.

[87] F. Ayaz, Z. Sheng, I. W.-H. Ho, D. Tiany, and Z. Ding, “Blockchain-enabled FD-NOMA based vehicular network with physical layer security,” in *2022 IEEE 95th Vehic. Technol. Conf.: (VTC2022-Spring)*, Jun. 2022, pp. 1–16. doi: 10.1109/VTC2022-Spring54318.2022.9860421.

[88] D. Das, S. Banerjee, P. Chatterjee, U. Ghosh, and U. Biswas, “A secure blockchain enabled V2V communication system using smart contracts,” *IEEE Trans. Intell. Transp. Syst.*, vol. 24, no. 4, pp. 4651–4660, Apr. 2023. doi: 10.1109/TITS.2022.3226626.

[89] A. Devi, G. Rathee, and H. Saini, “Secure blockchain-internet of vehicles (B-IoV) mechanism using DPSO and M-ITA algorithms,” *J. Inf. Secur. Appl.*, vol. 64, no. 3, Feb. 2022, Art. no. 103094. doi: 10.1016/j.jisa.2021.103094.

[90] R. Khan, A. Mehmood, Z. Iqbal, C. Maple, and G. Epiphaniou, “Security and privacy in connected vehicle cyber physical system using zero knowledge succinct non interactive argument of knowledge over blockchain,” *Appl. Sci.*, vol. 13, no. 3, Feb. 2023, Art. no. 1959. doi: 10.3390/app13031959.

[91] A. L. Shrivastava and R. K. Dwivedi, “Designing a secure vehicular internet of things (IoT) using blockchain: A review,” in *First Int. Conf. Adv. Comput. Future Commun. Technol. (ICACFCT)*, Dec. 2021, pp. 225–230. doi: 10.1109/ICACFCT53978.2021.9837373.

[92] S. Sunilkumar and S. Tangade, “Blockchain-based authentication and trust computation security solution for internet of vehicles (IoV),” in *Applications of Blockchain and Big IoT Systems*. Apple Academic Press, 2022.

[93] S. Smys and H. Wang, “Security enhancement in smart vehicle using blockchain-based architectural framework,” *J Artif. Intell. Capsule Netw.*, vol. 3, no. 2, pp. 90–100, Jun. 2021. doi: 10.36548/jaicn.2021.2.002.