A Review on Blockchain Technologies for Cyber-Resilient Automotives

Vaishnavi Rao[1], Prerana Cheguru[2], Delicia Fernandes[3], Sharani Regonda[4], and Pooria Yaghini[5]

Department of Computer Science, California State University Long Beach, *pooria.yaghini@csulb.edu*

{vaishnavi.rao01,prerana.cheguru01,deliciadomnic.fernandes01,sharani.regonda}@student.csulb.edu

ABSTRACT

As automotive technologies evolve to include advanced connectivity, automation, and electrification, cybersecurity threats pose greater risks that can undermine safety. While current automotive architectures implement cybersecurity controls, additional assurance is required to ensure cyber resilience, especially with increasing integration with the Internet of Things (IoT). Blockchain has emerged as a decentralized approach to developing trustworthy distributed systems resilient to cyber-attacks. This paper reviews blockchain platforms and protocols for enabling cyber-resilient automotive solutions within the context of Intelligent Transportation Systems (ITS). We analyze key blockchain properties including consensus algorithms, smart contracts, access controls, and privacy mechanisms. We also examine blockchain projects aimed at the automotive industry for vehicle-to-everything (V2X) communications, electric vehicle charging, and autonomous transactions.

Furthermore, we discuss the role of edge computing in meeting real-time and scale requirements for blockchain in vehicular systems. While blockchain delivers cybersecurity benefits, we outline challenges related to latency, standardization, governance, and adoption. As connected, electric, and autonomous vehicles become pervasive, blockchain can potentially provide inherent cyber resilience to keep pace with growing threats in an IoT ecosystem. With appropriate edge computing integration, blockchain systems for next-generation automotive solutions can be designed for security, safety, and sustainability.

Keywords: Blockchain, Internet of Things (IoT), cybersecurity, Intelligent Transportation Systems (ITS), smart contracts, vehicle-to-everything (V2X), automotive industry, edge computing

1. INTRODUCTION

The automotive industry is undergoing rapid transformation with the emergence of connected, autonomous, shared, and electric vehicles. These advances are enabled by integration with the Internet of Things (IoT), allowing real-time communication between vehicles and infrastructure through wireless networks [1]. However, connectivity exposes automotives to cybersecurity threats that can undermine safety. Recent attacks demonstrate vulnerabilities in telematics, infotainment systems, and critical components that can be exploited remotely [2]. As automotive technologies continue to advance, cybersecurity is paramount to ensure resilience against malicious threats in an increasingly connected ecosystem [3].

Blockchain has gained significant attention as a decentralized approach to developing secure distributed systems that are resilient to cyber-attacks [4]. A blockchain network relies on cryptographic functions and a consensus protocol run by distributed nodes to enable tamper-proof transactions without a central authority. Key properties including transparency, provenance, immutability, and consensus make blockchain highly robust against different cyber threats [5]. These characteristics can bolster integrity and trust in connected vehicles to prevent remote exploitation. Several blockchain platforms have emerged for IoT networks, providing capabilities that can be leveraged for automotive use cases [6].

Recent blockchain initiatives target enhanced cybersecurity specifically for intelligent transportation systems (ITS) [7]. Vehicle-to-everything (V2X) communication encompasses real-time data exchange between vehicles (V2V), infrastructure (V2I), pedestrians (V2P), networks (V2N), and the grid (V2G) [8], [9]. Blockchain systems can secure V2X with public key infrastructure, access controls, and verification of transmitted data [10]. Additional automotive applications include electric vehicle charging transactions [11], autonomous payments [12], and automobile supply chain tracking [13]. To meet real-time constraints, edge computing paradigms are being paired with blockchains [14]. As connected autonomous electric vehicles continue permeating urban environments, blockchain systems with edge integration can provide inherent resiliency against cyber threats.

While blockchain delivers security benefits, there are notable challenges to address including latency, standardization across platforms, governance procedures, and enterprise adoption [15]. With careful system design, these concerns can be mitigated to fully harness the cybersecurity potential of blockchain for next-generation automotive technologies. As vehicles become increasingly connected in the IoT ecosystem, blockchain offers a promising approach to keeping pace with emerging threats while upholding safety and security.

2. BLOCKCHAIN AND CYBERSECURITY

As connectivity in vehicles continues growing rapidly, cybersecurity risks pose greater safety concerns [16]. Legacy automotive architectures utilized network segregation between critical driving systems and comfort features to minimize attack surfaces [17]. However, with increasing integration of telematics, infotainment and Wi-Fi hotspots, external interfaces offer more vulnerability vectors if not adequately protected [18]. Remote keyless entry systems have been compromised to steal vehicles, while commercial telematics devices were hacked to track vehicle locations and manipulate functionalities [19]. Furthermore, critical firmware vulnerabilities have enabled dangerous remote takeover of vital components like brakes and engines [20]. Such attacks clearly demonstrate the necessity for cyber-resilient automotive systems as connectivity exposes safety-critical elements.

While existing architectures implement cybersecurity controls including firewalls, intrusion detection and authentication using standards like ISO 21434, additional assurance is imperative [21]. As vehicles transform into cyber-physical systems with wide IoT integration, threats can have catastrophic physical impacts if malicious actors exploit vulnerabilities [22]. Legacy transportation infrastructure also poses interoperability challenges for connected self-driving cars, necessitating security across heterogeneous systems [23]. With autonomous capabilities, cyber attacks can endanger passengers and pedestrians if remotely manipulated at scale. Therefore holistic cybersecurity spanning vehicles, infrastructure and IoT ecosystems is paramount.

Blockchain delivers inherent security properties to enable resilient distributed applications, complementing conventional cyber protection controls [24]. Trustless consensus between nodes in a decentralized peer-to-peer network offers tamper-proof integrity for transactions through transparency and cryptography [25]. Using public key infrastructure, blockchain systems provide authentication, nonrepudiation and confidentiality while still maintaining availability against denial-of-service attacks [26]. Through decentralized trust rather than a central authority, blockchain resilience prevents single points of failure. Additionally, smart contracts allow trusted automation of complex processes through executable code stored immutably on-chain [27]. These capabilities suit securing automotive solutions integrated with IoT ecosystems against remote cyber threats.

Several blockchain projects now target automotive applications, yet most research has focused on financial transactions rather than cybersecurity [28]. Initial identity and access management solutions leverage blockchain for vehicle wallets, enabling authenticated V2X communications to prevent spoofing [29]. Further cryptography integrations across vehicles and traffic systems can ensure trusted data sharing essential for road safety [30]. Smart contract adoption has also emerged for electric vehicle charging requiring dynamic micropayments with providers [31]. Through consensus, edge computing and docker modularization, real-time constraints can be met for automotive blockchains [32]. While adoption remains limited, blockchain standardization and development initiatives indicate promising traction for cyber-resilient next-generation transportation [33].

A systematic methodology is necessary to determine appropriate blockchain selection factors for given automotive use cases [34]. With prolific growth of varied ledger architectures, consensus rules, privacy techniques and programming environments, thorough evaluations can pinpoint optimal configurations [35]. Both permissionless public blockchains and private consortium networks have particular advantages that suit different connectivity requirements across consumers and enterprises [36]. By examining automotive threat models, assets, stakeholders and business objectives in context of blockchain capabilities, purpose-built systems can enhance cyber resilience securely and efficiently [37]. A combination of conventional security controls with tailored blockchain integrations allows developing solutions resilient to emerging threats in the software-defined automotive IoT industry moving forward.

Blockchain stands as a cornerstone in the automotive sector, offering a secure and transparent foundation for managing extensive datasets. Its decentralized architecture serves as a robust defense, mitigating risks tied to single points of failure and unauthorized access. Smart contracts, seamlessly integrated into the automotive ecosystem, play a pivotal role in automating data validation processes and fortifying data integrity.

This integration empowers automotive manufacturers and cybersecurity experts, providing the tools to proactively detect anomalies, predict vulnerabilities, and swiftly address potential cyber threats. The use of machine learning and AI for analyzing vast datasets further enhances the strength of this collaborative system. As these advanced technologies delve into the intricacies of automotive operations, blockchain functions as an indelible ledger, recording every action taken. This immutable record not only fosters transparency but also establishes a resilient framework against evolving cybersecurity challenges.

The collaboration of blockchain and data analytics transcends conventional security measures, reshaping the cybersecurity landscape in modern automotive systems. This transformative partnership not only ensures the security of sensitive automotive data but also lays the foundation for a future where adaptability and resilience are inherent characteristics of cybersecurity practices [19][17].

2.1 VANETs and MANETs

In the realm of smart vehicles, the interplay between Vehicular Ad Hoc Networks (VANETs) and Mobile Ad Hoc Networks (MANETs) is pivotal for advancing intelligent transportation systems through real-time data exchange between vehicles (V2V) and infrastructure (V2I) [16]. The extensive data generated, covering traffic patterns, vehicle speeds, accidents, and environmental conditions, forms the bedrock of Big Data in VANETs and MANETs. When seamlessly integrated into smart vehicles, blockchain technology offers a secure and transparent framework for managing and validating these datasets.

Blockchain's decentralized nature, critical for data integrity and security, becomes especially relevant in handling sensitive information within intelligent transportation systems. Smart contracts, intrinsic to blockchain, automate data validation processes, reinforcing integrity in the context of smart vehicles. This integration empowers stakeholders to adeptly

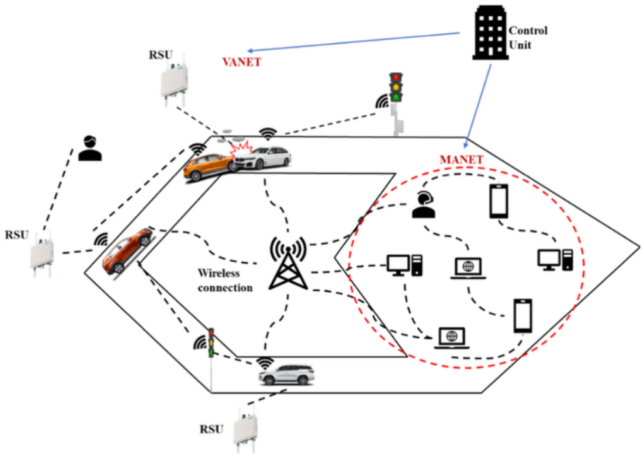

Figure 1: A comprehensive structure of Vehicular Ad-Hoc Network (VANET) and Mobile Ad-Hoc Network (MANET).

handle Big Data, ensuring the seamless deployment of secure and intelligent transportation systems. The strategic incorporation of blockchain into the symbiotic relationship of VANETs, MANETs, and Big Data analytics marks a transformative stride, shaping the future of smart vehicles where secure, transparent, and efficient data management becomes integral to a safer and optimized transport ecosystem [19][17].

3. BLOCKCHAIN AS A SOLUTION FOR AUTOMOTIVE SYSTEMS

As vehicles become more connected, electric, and autonomous, blockchain has emerged as an innovative solution to manage complex integrations. Core blockchain properties across decentralization, immutability, transparency and automation address pressing issues from security to efficiency across modern automotive systems. This section explores eight key areas where tailored blockchain implementations can enhance security, data integrity, innovation, privacy, scalability and more for the vehicles of tomorrow. Thoughtful blockchain systems hold vast potential to propel the automotive ecosystem into the future.

3.1 Decentralization and Enhanced Security

The concept of decentralization in blockchain is pivotal for enhancing security in automotive systems. Operating on a peer-to-peer network, blockchain distributes data across multiple nodes, mitigating the risk of centralized data breaches and single points of failure. This architecture transforms the automotive ecosystem by dispersing information, making it more resilient to potential attacks. In this decentralized framework, compromising the integrity of the network becomes significantly more challenging for attackers. The distributed nature of blockchain not only safeguards sensitive data but also fortifies the entire automotive infrastructure against potential vulnerabilities, providing a robust defense mechanism in the face of evolving cybersecurity threats [17].

3.2 Immutability and Data Integrity

The immutability of blockchain records is a cornerstone, rendering data alteration nearly impossible once recorded [17][18]. This characteristic holds significant implications for automotive systems where maintaining accurate service records and vehicle history is paramount. In the context of vehicle-to-vehicle (V2V) communication, ensuring the reliability of transmitted data and and V2I infrastructure is critical. Blockchain's unalterable nature provides a robust foundation for preserving the integrity of information vital to the performance, maintenance, and inter-vehicular communication within the automotive ecosystem.

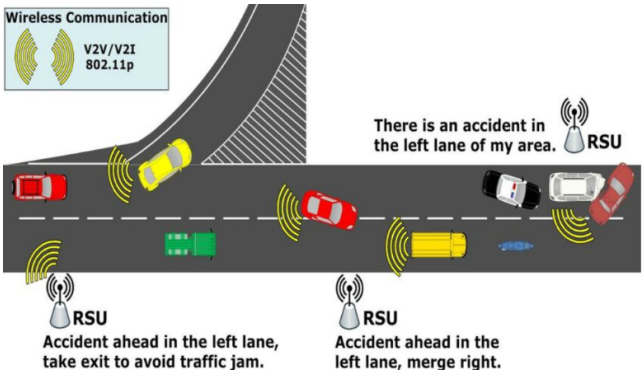

Figure 2: Real-time data exchange between vehicles (V2V) and (V2I) infrastructure.

In automotive systems, blockchain's unalterable records, once data is recorded, ensure an unparalleled level of data integrity [17][18]. This immutability proves crucial for maintaining accurate service records, preserving comprehensive vehicle histories, and ensuring the reliability of vehicle-to-vehicle (V2V) communication. The ability to trust the integrity of recorded information is foundational for the seamless operation and safety of smart vehicles, contributing to a resilient and trustworthy automotive infrastructure.

3.3 Transparency and Traceability

Blockchain's transparent nature, allowing all network participants to view and verify data, fosters trust among stakeholders [17][18]. In automotive systems, transparency is crucial for ensuring the reliability of data related to vehicle performance, maintenance, and communication within the vehicular network. Additionally, blockchain contributes to the traceability of automotive parts in the supply chain, facilitating the tracking of components from manufacturing to installation. This traceability ensures authenticity, compliance with safety standards, and establishes a verifiable record of each component's journey, promoting accountability in the automotive industry

3.4 Data Privacy with Pseudonymization

In blockchain systems, the delicate balance between transparency and privacy necessitates attention to privacy concerns [18]. Addressing this inherent tension becomes imperative, especially in the context of sensitive data within automotive systems. Pseudonymization emerges as a crucial technique employed by blockchain to mitigate privacy risks. This approach involves substituting identifiable information with pseudonyms, safeguarding user identities while preserving

the integrity of transaction history. Blockchain's utilization of pseudonymization techniques not only upholds privacy standards but also ensures that the transparent and traceable nature of the technology is harnessed responsibly, fostering a secure and privacy-respecting environment within the dynamic landscape of automotive data management.

3.5 Consensus Mechanisms for Reliability

Blockchain relies on consensus mechanisms to validate and agree upon transactions. Notable mechanisms include Proof of Work (PoW) and Proof of Stake (PoS). PoW involves nodes solving complex mathematical puzzles to validate transactions, ensuring security but demanding substantial computational power. PoS, conversely, selects validators based on their stake in the network, offering energy efficiency but potentially raising centralization concerns. Choosing the right consensus mechanism is critical for automotive applications. The efficiency and scalability of PoW make it reliable for maintaining the integrity of vast automotive datasets, but energy consumption concerns may arise. PoS, with its energy efficiency, suits scenarios where speed is crucial, ensuring reliability in real-time processes like autonomous vehicle communication. Striking a balance between security, efficiency, and scalability is pivotal when integrating consensus mechanisms into the fabric of automotive systems [17].

3.6 Integration with Other Technologies

Blockchain's integration with IoT devices and AI systems in vehicles amplifies data processes [18]. This seamless fusion enhances data collection, analysis, and decision-making within automotive systems. Beyond efficiency gains, blockchain paves the way for advanced automotive features. From enabling autonomous driving through secure and transparent data exchange to facilitating predictive maintenance based on real-time, immutable records, blockchain propels the automotive industry toward innovation. The potential also extends to personalized in-vehicle experiences, demonstrating how the harmonious integration of blockchain with IoT and AI technologies augments not only operational aspects but also the overall capabilities and user experiences within the dynamic landscape of smart vehicles.

3.7 Addressing Scalability and Energy Efficiency

Blockchain encounters scalability challenges, especially relevant in handling the substantial data generated by modern vehicles [17]. To address this, recent advancements and innovative solutions strive to enhance blockchain's scalability and energy efficiency, ensuring its suitability for automotive applications. Proposed strategies include off-chain transactions, layer-two scaling solutions ,and consensus algorithm enhancements. These endeavors aim to overcome the limitations associated with blockchain scalability, fostering a more adaptable and energy-efficient framework capable of accommodating the data-intensive nature of automotive systems. These developments mark crucial steps in optimizing blockchain technology for the dynamic and expansive requirements posed by the ever-evolving landscape of smart vehicles.

4. KEY FEATURES OF BLOCKCHAIN FOR AUTOMOTIVES

4.1 Enhanced Security through Cryptography

Blockchain's commitment to enhanced security is rooted in the utilization of robust cryptographic algorithms. Each transaction within the blockchain is meticulously encrypted and intricately linked to the preceding one, forming an immutable and secure chain of data [17]. This foundational reliance on advanced cryptographic techniques ensures the confidentiality and integrity of the information exchanged. In the context of automotive security, this feature assumes critical significance, particularly in the realm of connected and autonomous vehicles. The encryption of every transaction becomes a formidable defense against potential hacking attempts and unauthorized access to sensitive data. The integration of sophisticated cryptographic measures within blockchain establishes a resilient framework, fortifying the confidentiality and security of data, thus ensuring the trustworthiness and integrity of connected automotive systems.

4.2 Decentralization for Resilience

The adoption of decentralized principles in blockchain, facilitated by Distributed Ledger Technology, stands as a paramount strategy for fortifying resilience in data management [18]. Unlike conventional centralized databases, blockchain strategically distributes data across a network of computers, eliminating the vulnerability associated with a single point of failure. This decentralization proves instrumental in enhancing system resilience, providing a robust defense against potential cyberattacks or technical failures. In the context of automotive systems, decentralization assumes heightened significance. By preventing large-scale failures or targeted attacks, it ensures the continuous and reliable operation of critical vehicular systems such as navigation, communication, and automated driving aids. The application of decentralized ledger technology in automotive networks not only safeguards against disruptions but also instills a foundation of reliability vital for the evolving landscape of connected and autonomous vehicles.

4.3 Transparency and Trust

Blockchain's commitment to transparency and trust is embodied in its open and transparent ledger, balancing visibility with privacy [16]. The technology ensures the security of transactions while offering a clear, visible, and verifiable ledger accessible to all participants. This transparency becomes a cornerstone in fostering trust within the automotive ecosystem. Manufacturers, suppliers, dealers, and customers benefit from an unambiguous record, particularly in critical aspects such as vehicle history, ownership transfers, and part authenticity. The open ledger not only serves as a testament to the integrity of transactions but also as a mechanism for enhancing accountability and credibility across the automotive supply chain. In this way, blockchain not only secures data but establishes a foundation of transparency that is indispensable for building trust and reliability within the intricate web of relationships in the automotive industry.

4.4 Immutability for Reliable Records

The concept of immutability in blockchain underpins the reliability of its records. Once data is recorded, it attains an unalterable status, safeguarded by the consensus mechanism inherent in the network [17]. This attribute assumes paramount importance in the context of smart vehicles, particularly in maintaining accurate and dependable vehicle histories. The immutability of blockchain records ensures the integrity of service records, ownership history, and transaction details. This, in turn, proves indispensable for factors such as resale value and adherence to safety compliance standards. By guaranteeing that recorded information remains unaltered, blockchain establishes a robust foundation for the creation and preservation of trustworthy and tamper-proof vehicle records, contributing to the overall reliability and credibility of the automotive ecosystem.

4.5 Smart Contracts for Efficiency and Automation

Smart contracts revolutionize efficiency and automation by enabling the automated execution of transactions based on predefined conditions, eliminating the need for intermediaries [16]. Within the automotive industry, the transformative potential of smart contracts manifests in the automation of diverse processes. From streamlining leasing procedures and automating payments to expediting insurance claims and facilitating automated toll payments, smart contracts introduce unprecedented operational efficiency. This automation not only minimizes the need for manual interventions but also mitigates the risk of errors associated with human processing. In the dynamic landscape of automotive operations, the integration of smart contracts emerges as a catalyst for increased efficiency, precision, and the seamless execution of transactions, heralding a new era in operational optimization.[18]

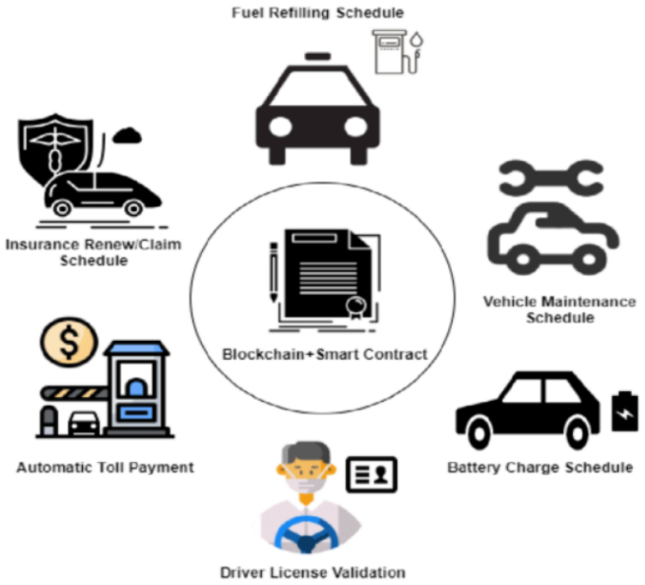

Figure 3: Execution of smart contracts for autonomous vehicles.

4.6 Interoperability and Integration

Blockchain platforms, leading the change in technological advancement, prioritize compatibility with various systems to facilitate seamless data exchange [16]. Their architecture is designed for interoperability, ensuring smooth integration with a diverse range of technologies and fostering collaboration across the digital landscape. In the automotive industry, this interoperability proves particularly advantageous. As blockchain seamlessly combines with IoT devices and AI systems within vehicles, it establishes a cooperative ecosystem. This synergy facilitates advanced data analytics, empowering predictive maintenance efforts and enriching personalized user experiences. The ability of blockchain to seamlessly operate within the automotive sector transcends conventional limitations, creating a dynamic environment where interconnected systems work together cohesively, offering limitless possibilities for technological progress and heightened operational capabilities [19].

5. USE-CASES OF BLOCKCHAIN IN THE AUTOMOTIVE INDUSTRY

Based on the automotive industry, here are several use cases for blockchain technologies in cyber-resilient automotives:

5.1 Vehicle-to-Vehicle (V2V) Communication

Blockchain can secure V2V communication by using a decentralized network that ensures data integrity and prevents unauthorized access or fraudulent communications, as explored by Lu et al. and Choi et al. [1][8].

5.2 Vehicle-to-Infrastructure (V2I) Interaction

As mentioned by Cui et al., blockchain can facilitate secure and efficient interactions between vehicles and road infrastructure, improving traffic management and road safety [7].

5.3 Supply Chain Transparency

Blockchain provides traceability in the supply chain, allowing for the verification of the authenticity and origin of automotive parts, as discussed by Korpela et al. [13].

5.4 RSecure Firmware Updates

The secure distribution of firmware updates can be managed through blockchain, mitigating the risk of tampering as vehicles increasingly become connected, as highlighted by Zhao and Ge [3].

5.5 Decentralized Charging Networks for Electric Vehicles

Blockchain can enable peer-to-peer energy trading among electric vehicles, creating a decentralized network for electric vehicle charging as researched by Kang et al. [9].

5.6 Smart Contracts for Automated Transactions

Smart contracts can automate transactions related to toll payments, parking fees, and vehicle sharing, as described by Christidis and Devetsikiotis [6].

5.7 Data Privacy and Security

Integrating blockchain into the automotive IoT can enhance data privacy and security, safeguarding against unauthorized access and cyber threats, as demonstrated in the case study by Dorri et al. [10].

5.8 Vehicle-to-Manufacturer (V2M) Data Sharing

Blockchain enables secure sharing of vehicle data with manufacturers for maintenance and diagnostics without compromising privacy, as explained by Sedghi et al. [11].

5.9 Enhanced Cybersecurity Measures

Addressing the cybersecurity needs of connected and autonomous vehicles through blockchain-based systems to resist sophisticated cyber-attacks, as discussed by Asokan and Tse et al. [16][17].

5.10 Regulatory Compliance

Blockchain systems can help ensure compliance with global regulations by providing immutable records of all transactions and interactions, which could be beneficial for audit and compliance purposes [21][22].

5.11 Identity Management

Blockchain can provide robust identity management solutions for vehicles, ensuring that communication and transactions are authenticated, as explored by Conoscenti et al. [4].

5.12 IoT Device Management

The integration of blockchain in managing IoT devices within vehicles can ensure secure and efficient device management, as researched by Viriyasitavat et al. [14].

These use cases underscore the versatility and potential of blockchain technologies to address various aspects of cybersecurity and resilience in the rapidly evolving automotive industry.

6. COMPARATIVE ANALYSIS

A comparative analysis of the provided references suggests a multi-faceted approach to the implementation of blockchain technology in the automotive industry, focusing on cyber-resilience. Here's an analysis based on the various themes and contributions of the cited works:

6.1 Consensus Protocols and Security

Lu et al. [1] and Zheng et al. [5] discuss the foundational aspects of blockchain consensus protocols, highlighting their critical role in maintaining the security and integrity of the distributed ledger. Zheng et al. further elaborate on different consensus algorithms, which are essential for cyber-resilient automotive solutions.
Choi et al. [8] delve into cooperative secure communications, which can be applied to V2V interactions. Their work suggests that security can be enhanced by blockchain, but the consensus mechanism needs careful selection to balance between efficiency and security.

Stakeholder	Specific challenges
Car owners and lenders / buyers and sellers of pre-owned cars [127]–[129]	1) Lack of transparency regarding the car's history 2) Unpredictable car maintenance and repair costs 3) Lack of trust in the outcome of maintenance and repair jobs 4) Absence of informed buying options 5) Absence of car insurance options 6) Lack of trust in autonomous vehicles and IoT-connected vehicles 7) High-level transactional experience to consumers whilst reducing the costs incurred by them
Fleet management companies / Car leasing or sharing (car-sharing, ride-sharing or ride-hailing) companies [120], [130]	1) Lack of transparency regarding the car's history 2) Unpredictable car maintenance and repair costs 3) Lack of trust in the outcome of maintenance and repair jobs 4) Lack of interoperability with business partners 5) High operational costs, low margin 6) High costs in the car-sharing, ride-sharing and ride-hailing economy 7) Lack of trust in autonomous vehicles and IoT-connected vehicles
Car-sharing, ride-sharing or ride-hailing passengers [131], [132]	1) More affordable car rides 2) Better maintained cars 3) Lack of trust in autonomous vehicles and IoT-connected vehicles 4) Lack of a common mobility provider platform 5) Lack of instant payment
Car entrepreneurs [122], [130]	1) Expensive rates for car leasing and rental 2) Lower car-sharing, ride-sharing or ride-hailing partnership fees 3) Difficulties to set up business, unfair competition 4) Lack of trust in autonomous vehicles and IoT-connected vehicles 5) Lack of information sharing
Car dealers and retailers [122], [133], [134]	1) Updated car ownership records 2) Updated repair and maintenance records 3) Updated purchase records 4) Lack of trust in autonomous vehicles and IoT-connected vehicles 5) Lack of information sharing
OEM / Car manufacturers and suppliers [118], [122], [134]–[137]	1) Huge warranty claim costs 2) Enforcement of recommended maintenance and repair prices on the dealers 3) Customer complaints due to car dealers' violation of recommended maintenance prices set by car manufacturers 4) Lack of control of the car maintenance performed by authorized dealers 5) Weak customer loyalty 6) Cyber-attacks, system failure risks and enhanced security in autonomous vehicles and IoT-connected vehicles 7) Control of the logistics 8) Lack of information sharing
Insurance companies [138]–[140]	1) Inflexible and non-customized policy pricing 2) 5-10% of all claims worldwide are fraudulent [143] 3) Costly and inefficient claim management 4) Inaccurate customer policy pricing 5) Lack of oversight over the quality and pricing for a collision repair
Independent repair shops [129], [134]	1) Underutilized capacity 2) Customer retention 3) Low margins 4) Lack of brand confidence
After-market (producers, distributors and retailers of spare parts, garages) [134]	1) Inefficient stock management 2) Market for counterfeit spare parts 3) Lack of transparency in warranty monitoring and enforcement 4) Low margins 5) Lack of brand confidence

Figure 4: Summary comparison of previous survey articles on the A Review on Blockchain Technologies for an Advanced and Cyber-Resilient Automotive Industry.

6.2 Vehicle Communication Systems

Zhao and Ge [3] present a survey on the Internet of Vehicles (IoV), emphasizing the importance of seamless communication for connected vehicles. Blockchain, as Cui et al. [7] describe, can be an enabling technology for secure communication in intelligent transportation systems, offering a comparative advantage over traditional systems due to its inherent security features
Miller and Valasek [2] expose vulnerabilities in vehicle communication systems that blockchain could potentially address, as it provides a more robust framework for authentication and authorization than existing systems.

6.3 Smart Contracts and IoT

Christidis and Devetsikiotis [6] discuss how smart contracts and blockchain can transform IoT applications, including automotive systems, by automating processes and reducing the need for intermediaries. This automation capability is also echoed by Griggs et al. [15] who emphasize the potential for smart contracts in remote monitoring, a concept that can be extended to vehicle diagnostics and maintenance.

6.4 Energy Efficiency and Electric Vehicles

Kang et al. [9] focus on blockchain applications for energy trading among electric vehicles. This peer-to-peer trading model can be further enhanced by energy-efficient consensus

protocols like Proof of Stake, which, as Zheng et al. [5] suggest, may become dominant in automotive blockchain applications due to their lower energy requirements.

6.5 Supply Chain Management

Korpela et al. [13] describe how blockchain can be integrated into digital supply chains, offering enhanced traceability and transparency. This can be compared to the secure and efficient management of automotive supply chains, where the authenticity and origin of parts are critical.

6.6 Cybersecurity Threats and Solutions

Asokan [16] and Tse and Wang [17] provide insights into the cybersecurity ecosystem for connected vehicles, identifying various threats and countermeasures. Blockchain's role in mitigating these threats is comparative in its decentralized nature, which is less susceptible to single points of failure. Amoozadeh et al. [18] and Yan and Xu [21] both explore the security vulnerabilities in connected vehicles, with blockchain offering a comparative advantage by enabling a secure, tamper-proof method for updating and maintaining vehicle software and firmware.

6.7 Regulations and Standards

Sun et al. [22] highlight the need for security and privacy in connected intelligent transportation systems, which requires a global regulatory approach. Blockchain's ability to provide an immutable audit trail can aid in meeting regulatory compliance, offering a comparative benefit over traditional databases.

In summary, the comparative analysis reveals that blockchain technology offers several advantages over conventional systems in terms of security, transparency, and efficiency. The references collectively emphasize the transformative potential of blockchain across different aspects of automotive systems, from improving V2V and V2I communication security to enabling new business models like peer-to-peer energy trading and enhancing supply chain management. However, the consensus is that there is a need for tailored blockchain solutions that address the specific requirements of the automotive industry, including scalability, real-time processing, and integration with existing automotive technologies.

7. FUTURE WORK

Convergence: As vehicles increasingly interact with external entities, we foresee a future where cars directly transact with banks and power grids. This convergence demands interoperable blockchain solutions that integrate seamlessly with various industries [11][13].

Consensus Protocols: The dominance of energy-efficient mechanisms, such as Proof-of-Stake, in automotive blockchain applications is likely, given the need for sustainability and efficiency in vehicular networks [32].

Security: With the advent of quantum computing, there is an urgent need for blockchain security mechanisms that can withstand new levels of computational power, ensuring the integrity and security of automotive systems [17][21].

IoT and AI: The integration of IoT and AI within automotive systems will enable vehicles to make data-driven decisions. Logging these decisions on blockchains ensures transparency and accountability [18][24].

Identity: Decentralized identity solutions offer promising avenues for novel insurance models, such as user-based models, which align more closely with individual usage patterns and risk profiles [29].

Regulations: The development of tailored global rules and standards specifically for the use of blockchain in automotive applications is anticipated, addressing unique challenges and opportunities in this sector [21][23].

Transparency: Blockchain can enhance transparency in the automotive industry, enabling users to trace the origin of materials used in their vehicles and understand their ecological footprint [33].

Peer-to-Peer: The use of blockchain in facilitating direct car sharing or data exchanges can make these processes more efficient and cost-effective, bypassing traditional intermediaries [9][30].

Smart Contracts: Smart contracts are expected to evolve to manage dynamic and complex agreements, especially in scenarios like automated toll payments and dynamic insurance policies [26][27].

AR and VR: Blockchain can power virtual automotive experiences, leveraging AR and VR technologies for enhanced user engagement and training scenarios [14].

Green Blockchain: Prioritizing sustainability in blockchain operations is essential, particularly in the context of electric vehicles and the broader goal of reducing the carbon footprint of blockchain technologies [32].

Redefining Mobility: The fusion of blockchain and automotive technologies is set to redefine our mobility future, offering unprecedented levels of security, efficiency, and user-centricity in transportation [7][34].

These future work areas, anchored by blockchain technology, highlight a transformative phase in the automotive industry, steering towards enhanced cybersecurity, efficiency, and sustainability.

CONCLUSION

This comprehensive exploration into the integration of blockchain technology within the automotive sector, particularly in the context of Intelligent Transportation Systems (ITS), highlights blockchain's potential to significantly enhance cyber-

security. As vehicles become increasingly connected and autonomous, the necessity for robust cybersecurity measures intensifies. Blockchain's unique characteristics – decentralization, immutability, transparency, and the use of smart contracts – make it an ideal candidate for addressing these emerging challenges.

The study underscores blockchain's capacity to reinforce cybersecurity in automotive applications, from vehicle-to-everything (V2X) communications to electric vehicle charging and autonomous transactions. The role of edge computing in complementing blockchain to meet real-time and scalability requirements in vehicular systems is particularly noteworthy. However, the paper also acknowledges the challenges associated with blockchain adoption in the automotive sector, including issues related to latency, standardization, governance, and widespread acceptance.

Moving forward, it is imperative to address these challenges to fully leverage blockchain's potential for cybersecurity in the automotive industry. Future research should focus on optimizing blockchain implementations for reduced latency, developing standardized protocols for wider adoption, and formulating effective governance models that facilitate integration while ensuring security and privacy.

REFERENCES

1 N. Lu, N. Cheng, N. Zhang, X. Shen, and J. W. Mark, "Connected Vehicles: Solutions and Challenges," in IEEE Internet of Things Journal, vol. 1, no. 4, pp. 289-299, Aug. 2014. doi: 10.1109/JIOT.2014.2327587.

2 C. Miller and C. Valasek, "Remote Exploitation of an Unaltered Passenger Vehicle," Black Hat USA, 2015.

3 K. Zhao and L. Ge, "A Survey on the Internet of Vehicles," in Proceedings of the 2018 International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services, New York, NY, 2018. doi: 10.1145/3286978.3287010.

4 M. Conoscenti, A. Vetrò, and J. C. De Martin, "Blockchain for the Internet of Things: A systematic literature review," 2016 IEEE/ACS 13th International Conference of Computer Systems and Applications (AICCSA), Agadir, 2016, pp. 1-6. doi: 10.1109/AICCSA.2016.7945790.

5 Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends," 2017 IEEE International Congress on Big Data (BigData Congress), Honolulu, HI, 2017, pp. 557-564. doi: 10.1109/BigDataCongress.2017.85.

6 K. Christidis and M. Devetsikiotis, "Blockchains and Smart Contracts for the Internet of Things," in IEEE Access, vol. 4, pp. 2292-2303, 2016. doi: 10.1109/ACCESS.2016.2566339.

7 L. Cui, W. An and Q. Wu, "Application of Blockchain in Intelligent Transportation Systems and Smart Cities: An Overview," in IEEE Transactions on Intelligent Transportation Systems, doi: 10.1109/TITS.2021.3131391.

8 H. Choi, L. Dai, and W. Saad, "Wireless Powered Cooperative Secure Communications With Blockchains for Internet of Vehicles," in IEEE Transactions on Vehicular Technology, vol. 69, no. 6, pp. 6076-6090, June 2020. doi: 10.1109/TVT.2020.2987258.

9 J. Kang, R. Yu, X. Huang, S. Maharjan, Y. Zhang and E. Hossain, "Enabling Localized Peer-to-Peer Electricity Trading Among Plug-in Hybrid Electric Vehicles Using Consortium Blockchains," in IEEE Transactions on Industrial Informatics, vol. 13, no. 6, pp. 3154-3164, Dec. 2017. doi: 10.1109/TII.2017.2709784.

10 A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, "Blockchain for IoT security and privacy: The case study of a smart home," 2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops), Kona, HI, 2017, pp. 618-623. doi: 10.1109/PERCOMW.2017.7917634.

11 A. Sedghi, M. H. Cintuglu, O. A. Mohammed and O. A. Mohammed, "Blockchain technology for inter-domain collaborative intelligent transportation systems," 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), Halifax, NS, Canada, 2018, pp. 1030-1037. doi: 10.1109/Cybermatics 2018.2018.00211.

12 X. Huang, R. Yu, J. Kang, Z. Xia and Y. Zhang, "Software Defined Networking for Energy Harvesting Internet of Things: A Prospective Study," in IEEE Internet of Things Journal, vol. 5, no. 4, pp. 2300-2310, Aug. 2018. doi: 10.1109/JIOT.2018.2827219.

13 K. Korpela, J. Hallikas and T. Dahlberg, "Digital Supply Chain Transformation toward Blockchain Integration," Proceedings of the 50th Hawaii International Conference on System Sciences, 2017. doi: 10.24251/hicss.2017.506.

14 W. Viriyasitavat, L. D. Xu, Z. Bi, and D. Hoonsopon, "Blockchain Technology for Applications in Internet of Things - Mapping From System Design Perspective," in IEEE Internet of Things Journal, vol. 6, no. 5, pp. 8155-8168, Oct. 2019. doi: 10.1109/JIOT.2019.2920987.

15 K. N. Griggs, O. Ossipova, C. P. L. Kohlios, A. N. Baccarini, E. A. Howson and T. Hayajneh, "Healthcare Blockchain System Using Smart Contracts for Secure Automated Remote Patient Monitoring," in JMIR Medical Informatics, vol. 6, no. 7, 2018. doi:10.2196/10430.

16 N. Asokan, "Exploring Autonomous Vehicle Cybersecurity," IEEE Computer, vol. 51, no. 12, pp. 20-21, 2018. doi: 10.1109/MC.2018.2884131.

17 Y. T. Tse and S. S. Wang, "The Security Ecosystem for Connected Vehicles: Threats, Attacks, Simulation, and Countermeasures," Computer, vol. 55, no. 8, pp. 47-55, 2022. doi: 10.1109/MC.2021.3117418.

18 C. Amoozadeh, A. Raghuramu, C.-N. Chuah, D. Ghosal, H. M. Zhang, J. Rowe, and K. Levitt, "Security vulnerabilities of connected vehicle streams and their impact on cooperative driving functions and autonomy," 2015 IEEE 18th International Conference on Intelligent Transportation Systems, 2015, pp. 562-567. doi: 10.1109/ITSC.2015.131.

19 T. Hoppe, S. Kiltz, and J. Dittmann, "Security threats to automotive CAN networks – Practical examples and selected short-term countermeasures," Computer Safety, Reliability, and Security, pp. 235–248, 2008. doi: 10.1007/978-3-540-87698-4 21.

20 K. Koscher, A. Czeskis, F. Roesner, S. Patel, T. Kohno, S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, and S. Savage, "Experimental security analysis of a modern automobile," 2010 IEEE Symposium on Security and Privacy, 2010, pp. 447-462. doi: 10.1109/SP.2010.34.

21 G. Yan and W. Xu, "Cyberattack and Defense for Intelligent and Connected Vehicles: An Overview," IEEE Internet Things J., vol. 8, no. 5, pp. 3278–3302, 2021. doi: 10.1109/JIOT.2020.3013202.

22 Y. Sun, L. Wu, S. Li, B. Chen, B. Cheng, S. Zhang, and J. Lv, "Security and Privacy of Connected Intelligent Transportation System," IEEE Internet Things J., vol. 8, no. 7, pp. 5122-5141, 2021. doi: 10.1109/JIOT.2020.3036158.

23 M. Amoozadeh, A. Raghuramu, C-N. Chuah, D. Ghosal, H. M. Zhang, J. Rowe, and K. Levitt, "Security vulnerabilities of connected vehicle streams and their impact on cooperative driving functions and autonomy," 2015 IEEE 18th International Conference on Intelligent Transportation Systems, 2015, pp. 562-567. doi: 10.1109/ITSC.2015.131.

24 X. Liang, S. Shetty, D. Tosh, C. Kamhoua, K. Kwiat, and L. Njilla, "Towards data assurance and resilience in IoT using blockchain," 2017 IEEE Military Communications Conference (MILCOM), 2017. doi: 10.1109/MILCOM.2017.8170798.

25 N. Szabo, "Formalizing and securing relationships on public networks," First Monday, 1997. doi: 10.5210/fm.v2i9.548.

26 K. Christidis and M. Devetsikiotis, "Blockchains and Smart Contracts for the Internet of Things," IEEE Access, vol. 4, pp. 2292-2303, 2016. doi: 10.1109/ACCESS.2016.2566339.

27 G. Wood, M.E. Grady, J. Clark, and M.D. Dziembaj, "Ethereum: A secure decentralised generalised transaction ledger," Ethereum project yellow paper, vol. 151, pp. 1-32, 2014.

28 M. A. Khan and K. Salah, "IoT security: Review, blockchain solutions, and open challenges," Future Generation Computer Systems, vol. 82, pp. 395-411, 2018. doi: 10.1016/j.future.2017.11.022.

29 H. Choi, L. Dai, and W. Saad, "Wireless Powered Cooperative Secure Communications With Blockchains for Internet of Vehicles," IEEE Transactions on Vehicular Technology, vol. 69, no. 6, pp. 6076–6090, 2020. doi: 10.1109/tvt.2020.2987258.

30 J. Kang, R. Yu, X. Huang, S. Maharjan, Y. Zhang and E. Hossain, "Enabling Localized Peer-to-Peer Electricity Trading Among Plug-in Hybrid Electric Vehicles Using Consortium Blockchains," IEEE Transactions on Industrial Informatics, vol. 13, no. 6, pp. 3154-3164, 2017. doi: 10.1109/tii.2017.2709784.

31 A. Sedghi, M.H. Cintuglu, O.A. Mohammed, and O.A. Mohammed, "Blockchain technology for inter-domain collaborative intelligent transportation system," 2018 IEEE 8th Annual Computing and Communication Workshop and Conference (CCWC), 2018. doi: 10.1109/ccwc.2018.8301738.

32 W. Viriyasitavat, L.D. Xu, Z. Bi, and D. Hoonsopon, "Blockchain Technology for Applications in Internet of Things - Mapping From System Design Perspective," IEEE Internet of Things Journal, vol. 6, no. 5, pp. 8155-8168, 2019. doi: 10.1109/jiot.2019.2920987.

33 K. Korpela, J. Hallikas, and T. Dahlberg, "Digital Supply Chain Transformation toward Blockchain Integration," 2017 50th Hawaii International Conference on System Sciences, 2017. doi: 10.24251/hicss.2017.506.

34 M. Conoscenti, A. Vetrò and J. C. De Martin, "Blockchain for the Internet of Things: A systematic literature review," 2016 IEEE/ACS 13th International Conference of Computer Systems and Applications (AICCSA), 2016. doi: 10.1109/aiccsa.2016.7945790.

35 Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends," 2017 IEEE International Congress on Big Data, 2017. doi: 10.1109/bigdatacongress.2017.85.

36 K. Christidis and M. Devetsikiotis, "Blockchains and Smart Contracts for the Internet of Things," IEEE Access, vol. 4, pp. 2292-2303, 2016. doi: 10.1109/access.2016.2566339.

37 A. Dorri, S.S. Kanhere, R. Jurdak, and P. Gauravaram, "Blockchain for IoT security and privacy: The case study of a smart home," 2017 IEEE International Conference on Pervasive Computing and Communications Workshops, 2017. doi: 10.1109/percomw.2017.7917634.