Enhancing Trust and Transparency in Multi-Stakeholder Data Ecosystems via Blockchain: A Case of BC-4Track

BUSRA OZDENIZCI KOSE[1], VEDAT COSKUN[2], MIKAIL ABDULLAH ORAL[3]
[1]Department of Management Information Systems,
Gebze Technical University, Kocaeli,
TÜRKIYE

[2]Department of Software Engineering,
Istanbul Atlas University, Istanbul,
TÜRKIYE

[3]Turkcell Technology, Istanbul,
TÜRKIYE

Abstract: In today's increasingly interconnected world, organizations interact with complex data ecosystems that feature multiple independent stakeholders. Establishing trust, transparency, as well as integrity concerning such ecosystems is a difficult task, particularly if stakeholders feature conflicting interests with different, unintegrated information systems. Conventional, centrally managed systems are prone to single-point failures, manipulations, as well as delays within the verification process. Blockchain technology, with its decentralized, immutable system, provides a sound basis for addressing such issues. BC-4Track, a blockchain-enabled system, is presented as a solution that provides secure, transparent, as well as tamper-proof management of lifecycle information within the automotive industry. This system incorporates IoT-based smart kits for real-time information acquisition, Ethereum-based smart contracts for automated record management, as well as a web-based decentralized application (DApp) that enables stakeholder interaction. Thorough analyses were carried out with a focus on system functionality, system efficiency, and system reliability. System usability, system responsiveness, and system security were validated. These results demonstrate the applicability of blockchain-based solutions in such environments with multiple stakeholders, with regard to issues such as trust.

Key-Words: - Blockchain, Multi-Stakeholder, Data Management, Trust, Transparency, Vehicle Lifecycle Management, IoT Integration.

Received: June 12, 2025. Revised: August 26, 2025. Accepted: October 11, 2025. Published: May 14, 2026.

1 Introduction

In the modern interconnected economy, many sectors involve complicated ecosystems with multiple stakeholders, where the creation, sharing, and verification of essential information is most often a constant process carried out by manufacturers, service deliverers, authorities, and end-users [1], [2]. Maintaining integrity, transparency, and trust within such environments is increasingly being sought as a result of regulations that call for accountability and traceability across the globe. However, within such ecosystems with conflicting interests, varied systems, and the absence of a mutual verification system, issues related to the formation of data silos, authenticity disputes, and efficiency issues increase [2], [3]. Conventional systems, with their centralized models, increase such problems through single points of-failure, vulnerability to manipulations, as well as an inability for real-time authenticity verification [4], [5].

The automotive sector represents a particularly compelling example of such complexity. The lifecycle of a vehicle includes many stages (manufacturing, change of ownership, services, reporting of accidents, end-of-life processing) that provide many pieces of necessary information that can directly impinge upon claims, compliance, value, as well as assessment [6], [7], [8]. However, the fragmented record-keeping practices, as well as a lack of standardization in the area of interoperability, often give rise to some issues with the verification process, as well as a lack of integrity, thus establishing the importance of establishing a safe, shared, or verifiable record management system [9], [10].

Blockchain technology offers a promising solution to these challenges through its decentralized, tamper-resistant, and transparent ledger structure [11], [12]. By removing reliance on a single authority, blockchain enables secure and auditable data sharing between untrusted parties [13]. When complemented by supporting technologies such as IoT-based data acquisition, vehicle lifecycle events can be captured automatically, stored immutably, and made accessible in real time to authorized stakeholders [14]. This will address authenticity issues, simplify verification processes, and enhance authenticity.

BC-4Track, a blockchain-based system design for vehicle lifecycle management, was proposed in this work as a solution that would enhance trust, transparency, and efficiency in the automotive industry. The platform integrates an IoT-based Smart Kit for real-time vehicle data acquisition, Ethereum-based smart contracts for tamper-proof lifecycle event recording, and a web-based decentralized application (dApp) that provides stakeholders with a unified interface for submitting, verifying, and retrieving records. Built with interoperability and role-based access control at its core, BC-4Track ensures that authorized users -including manufacturers, insurers, rental companies, and regulatory bodies- can securely interact with lifecycle data according to their defined privileges. The prototype has undergone functional, unit, dynamic, and static analysis tests under various scenarios, demonstrating its ability to meet real-time operational requirements while maintaining high data integrity.

While blockchain has been applied in the automotive sector, prior studies often focus on isolated lifecycle segments -such as supply chain provenance or vehicle identity verification- and lack a holistic, multi-stakeholder architecture that integrates IoT-driven real-time event capture with on-chain verification. BC-4Track addresses this shortfall with its comprehensive, end-to-end solution that brings together on-vehicle incident data, verification through decentralized technology, and accessibility within a secure framework. Although the architecture was validated within the automotive industry, its design can be applicable in other industries that require trusted, real-time, and traceable data management. Such industries may include supply chain management, public service registry, or asset tracking.

The rest of this paper is outlined as follows: Section 2 briefly reviews the literature. Section 3 describes the system architecture. Section 4 presents the implementation. Section 5 provides the results, along with a discussion. Finally, Section 6 concludes with recommendations.

2 Related Work

Blockchain technology has been identified as a transformative solution to enhance aspects of trust, transparency, and integrity of the shared data within a scenario that consists of more than two independent parties [11], [12], [13], [14]. This technology provides a decentralized, immutable, and traceable method of record keeping, eliminating the use of centralized third-party services that may pose risks associated with single points of failure [15], [16]. However, the use of such technology in decentralized systems, such as multiple organizational networks that may pose different levels of interests with regard to the processing of shared decision information, seems more essential [15], [16]. Over the past decade, blockchain applications have expanded across domains such as sustainable supply chains [15], [16], healthcare [17], [18], public services [19], [20], and financial transactions [21], [22], offering varying degrees of decentralization and security.

In the field of multi-stakeholder collaboration, though, the use of blockchain technology solutions shows great promise for the improvement of trust management, as well as traceability. Specifically, within the realm of supply chain management, blockchain technology solutions have been used for purposes of guaranteeing traceability, secure record keeping, as well as the autonomous enforcement of contracts through smart contracts [9], [10], [23]. By implication, for example, sustainable models of supply chain management through the use of blockchain technology within the Industry 5.0 vision stress the importance of incorporating the use of distributed ledgers to promote traceability, accountability, and sustainability within a collaborative environment [15], [16]. Similarly, for example, within collaborative transport management, the use of blockchain technology solutions for trust management purposes promotes the use of role-based management, as well as tamper-proof logs within collaborative decision-making [24], [25]. However, as indicated, the use of such technology solutions still lacks full lifecycle management, particularly within applications that call for real-time verification, as well as collaborative interoperation.

From a vehicle centric perspective, existing literature in the Internet of Vehicles (IoV) technology space recognizes a relevant application scope for blockchain-enabled multi-stakeholder systems [22],

[23], [26]. Existing literature has assessed key requirements such as maintaining privacy for protected vehicular information through use of blockchain centric encryption and anonymization strategies [27], secure sharing of information across multiple vehicles through use of consortium based blockchains [23], [28], as well as the establishment of robust communications infrastructure for autonomous as well as IoV based vehicles [28], [29], [30]. Such existing studies clearly indicate the reliance of blockchain technology on its relevant capabilities that can address security issues, integrity, and trust within highly dynamic vehicular networks. However, most existing applications of IoV technologies stop within well-selected phases of their lifecycles, such as vehicle operation or in-vehicle services, with most applications largely ignoring traceability. In addition, most IoV-centric designs of blockchain technologies do not provide a unified, role-based infrastructure that permits the seamless interaction of all key stakeholders.

Although there has been development in IoV blockchain frameworks that promote safe communications as well as chosen information sharing, typically, such frameworks do not offer a unified, role-based space that effectively incorporates all key participants, such as manufacturers, service companies, regulatory authorities, and users, throughout the entire lifespan.

BC-4Track directly addresses this gap by delivering an integrated, permissioned blockchain platform designed for end-to-end lifecycle management. The system combines role-based access control, smart contract–driven event recording, and interoperable data structures to maintain verifiable traceability from manufacturing through decommissioning. In contrast to existing studies limited to specific operational stages, BC-4Track enables continuous multi-stakeholder engagement and real-time verification, meeting both the technical and organizational adoption factors identified in earlier research. The system has been validated through a functional prototyping process that assessed the system's performance, dependability, and usability within real-world multiple participant settings. BC-4Track brings together the transparency required within the supply chain with the security involved in vehicular communications through a flexible reference model, thus addressing the divide that exists between generic models of blockchain adoption as well as industry-centric solution sets.

3 System Architecture

BC-4Track utilizes a multi-layer architecture that brings together IoT-based data acquisition, record management through Blockchain, as well as a user-centric decentralized application. Thus, as shown in Figure 1, this layered architecture helps with modularity, scalability, and secure communications within system components, hence enabling secure, verifiable, and real-time tracking of the entire vehicle lifecycle.

At the foundation, the IoT Layer consists of a prototyped Smart Kit designed to emulate in-vehicle event generation. The kit captures relevant lifecycle data such as maintenance events, mileage updates, and status changes, and securely forwards the generated data for processing within the BC-4Track platform. The design is adaptable for integration with production-grade IoT devices in future deployments.

Blockchain Layer is built upon a network that utilizes the Ethereum system, with multiple nodes being run by different participants that form a synchronized, immutable ledger. As shown in Figure 1, each stakeholder -such as rental companies, insurance providers, and regulatory authorities- has its own node that keeps a copy of the same blockchain. This decentralized structure eliminates single points of failure and ensures that all parties have access to a consistent version of the truth. Smart contracts running on the Ethereum network provide automated functionality such as the verification of incoming event data, sending of notifications, and the execution of predefined rules, all without the use of intermediaries.

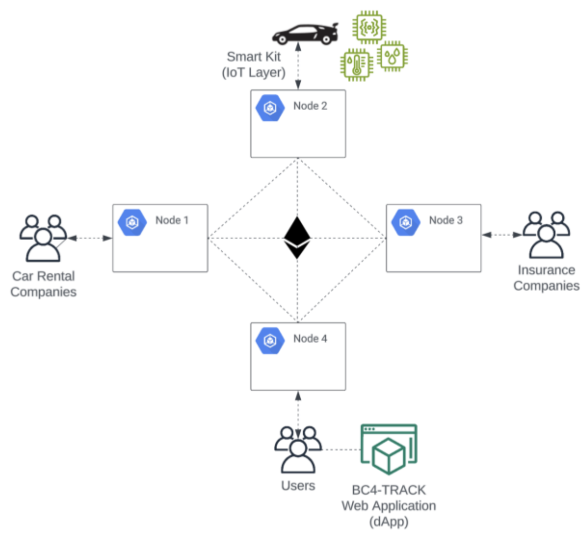


Fig. 1: System context
Source: created by the authors

The Application Layer is a web-based decentralized application (dApp) that serves as the primary interface for all participants. With this interface, users can record lifecycle events, query previous events, and ensure that the stored information is valid. The dApp communicates with blockchain nodes via Web3.js, with the backend taking care of storing additional information that is not required on the blockchain. Role-based access control ensures that authorized parties can only record or query any information.

Inter-layer communication follows a secure and standardized approach. Events generated by the Smart Kit are transmitted to the backend, where validation logic ensures compliance with predefined data formats. The validated data is then forwarded to the blockchain network through the smart contract interface. Conversely, data retrieval requests are routed through the dApp, which queries both the blockchain and off-chain storage as necessary to provide complete and accurate information to the requesting stakeholder.

This architecture has been designed to be hardware-agnostic, allowing future integration with production-grade IoT devices and alternative blockchain platforms. By combining decentralized data management with real-time IoT event acquisition, BC-4Track bridges the gap between conceptual blockchain frameworks and functional, demonstrable prototypes in the context of vehicle lifecycle management.

4 Implementation

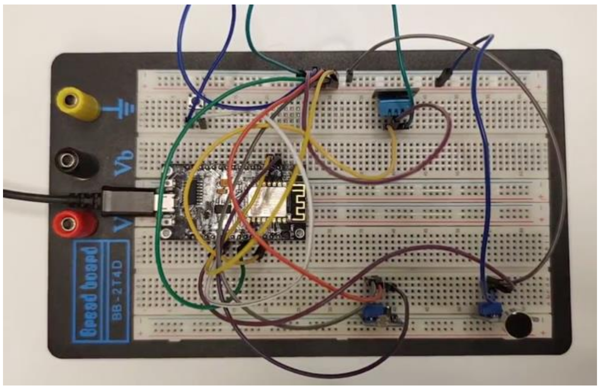
The BC-4Track platform was implemented using a combination of hardware prototypes, blockchain infrastructure, and a web-based dApp. A modular development approach was followed, enabling the independent design, testing, and deployment of each architectural layer -IoT, blockchain, and application- before full system integration. The blockchain layer was implemented on the Ethereum Sepolia test network through smart contracts that were designed using the Remix IDE with MetaMask functionality for signing and verification of the transactions. Backend solutions were developed using Node.js, with the frontend solution built with React along with Web3.js.

4.1 Smart Kit Development

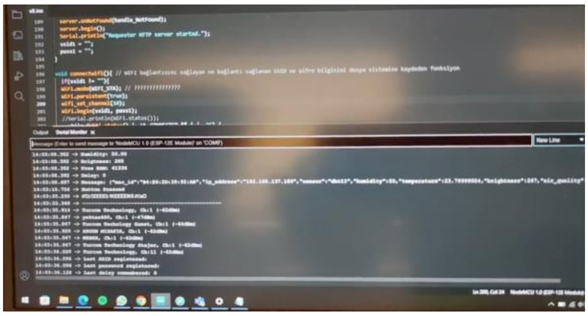
During the implementation, a Smart Kit was designed with the purpose of reading sensor data from vehicles as well as securely sending this information to the blockchain network. A NodeMCU microcontroller was used in the design of this prototype. This was linked with temperature as well as humidity sensors. To increase its applications, other modules such as air quality sensors, as well as light sensors, were also used (Figure 2-a). The device performs basic preprocessing before preparing the sensor readings for transmission and ensures that each event is captured in a consistent and verifiable structure.

Circuit prototyping was carried out using a BB-2T4D breadboard, allowing rapid and reliable assembly. Sensor readings were packaged in JSON format and transmitted via Wi-Fi to a local server application for initial testing (Figure 2-b). This server -representing the backend component in the BC-4Track architecture- validated and processed the incoming data before forwarding it to the blockchain network during integration testing. This design ensures that the Smart Kit operates as the primary IoT data acquisition module and links physical-world events with the digital ledger.

Testing confirmed stable operation and accurate real-time data transmission, demonstrating that the Smart Kit prototype met the functional requirements of the BC-4Track system and formed the core event acquisition component of its IoT layer.



(a)



(b)

Fig. 2: Smart kit development
Source: created by the authors

4.2 Blockchain Architecture and Integration

The blockchain component was deployed on the Ethereum Sepolia test network, configured as a permissioned multi-node environment for testing purposes. Smart contracts were developed in Solidity using the Remix IDE (Figure 3), integrated with MetaMask for transaction signing and verification. Each stakeholder node -representing entities such as rental companies, insurance providers, and regulatory authorities- maintains a synchronized copy of the distributed ledger. These contracts define event validation rules, automate lifecycle status updates, and enforce business logic without intermediaries.

Given the existing deployment scenario, the testing environment supports Ethereum Virtual Machine compatibility, stable block times, as well as a controlled environment that verifies the processing of transactions without any monetary costs or use of production data. However, for a real-world production deployment within a multiple-stakeholder automotive industry, a private or consortium-based blockchain would be more suitable. This is because private blockchains provide low latency, reduced overhead costs for processing transactions, as well as controlled regulation, while consortium blockchains provide support for shared policy compliance between manufacturers, service companies, insurance companies, and regulators. Therefore, permissioned blockchains are more desirable in production environments for their scalability, compliance, and reliability, whereas the existing configuration is sufficient for prototyping.

For interaction with the blockchain, the backend utilizes Web3.js. Also, a permission system based on roles is implemented to guarantee that only authorized participants may record or consult specific types of events related to the lifecycles of different vehicles.

Integration testing validated the correct recording of Smart Kit data across all network nodes, ensuring identical and immutable ledger copies. Performance evaluations confirmed consistent transaction finalization within acceptable latency for real-time tracking, while integrity checks verified that any tampering attempt was rejected by the network's consensus mechanism, ensuring tamper resistance.

Figure 3 illustrates the interaction with the deployed BC-4Track smart contract in the Remix IDE. Figure 3-a demonstrates the execution of set functions (e.g., *setOwner, setVehicle, setPolicy*) for adding new entities to the blockchain, while Figure 3-b shows the output of get functions (e.g., *getOwners, getVehicles, getPolicies*) used to retrieve stored lifecycle data. These interactions confirm the correct operation of both data entry and retrieval processes, ensuring the integrity and accessibility of on-chain records. While Figure 3 displays only a portion of the source code for illustration, the complete contract includes several helper functions that support event validation and lifecycle data management across owners, drivers, vehicles, accidents, policies, repairs, and services.

The smart contract utilizes a variety of inherent security measures that ensure the validity and integrity of all the lifecycle records stored within the blockchain. The *_validateString()* function performs input cleaning, rejecting blank or invalid string input, thus eliminating the possibility of submitting partially or falsely filled events. In addition, the *_isPlateExists()* method ensures that a vehicle plate is not repeated, thus eliminating the insertion of duplicate or conflicting information. More authorization verification is further necessary within the lifecycle method, thus requiring the *msg sender* authorization for accessing all privileged events, such as registering owners, storing events related to vehicle maintenance, or submitting accident events. Together, such mechanisms enforce strong data validation, integrity of the data between stakeholders, as well as the tamper-resistant, cryptographically verifiable nature of all lifecycle operations.

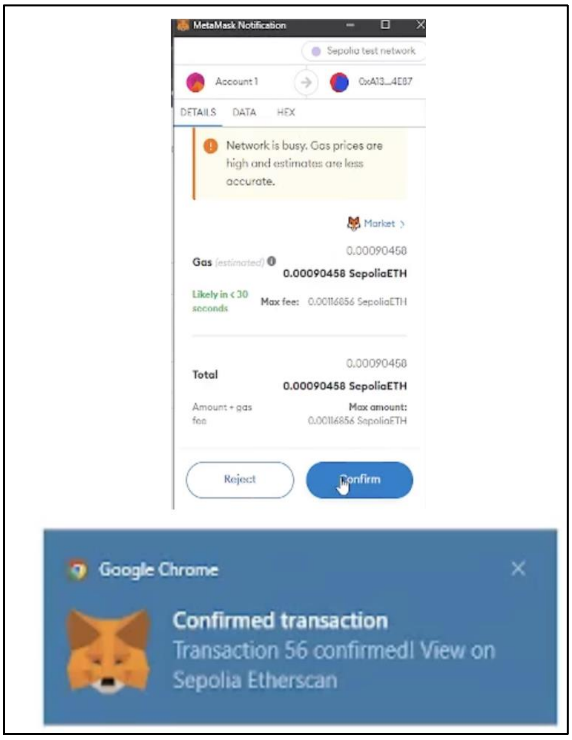
(a)

(b)

Fig. 3: Smart contract interaction in Remix IDE
Source: created by the authors

Additionally, Figure 4 illustrates the MetaMask integration employed during blockchain interactions. Figure 4-a presents the wallet connection prompt, which securely authenticates stakeholders before initiating any transaction. Figure 4-b depicts the transaction confirmation dialog, which allows users to review and approve lifecycle event submissions directly from their MetaMask wallet. This integration ensures that all blockchain operations -whether registering new entities or updating vehicle records- are cryptographically authorized by the respective stakeholder, thereby reinforcing the platform's role-based access control and safeguarding transaction integrity.

(a)



(b)

Fig. 4: MetaMask integration
Source: created by the authors

4.3 Application Layer and User Interface

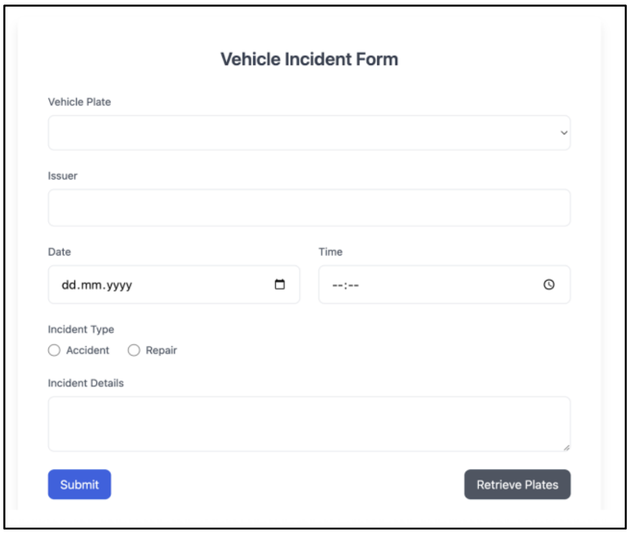
The BC-4Track application layer consists of a web-based decentralized application (dApp) that serves as the primary interaction point for stakeholders. With this interface, users will be able to record car events, check historical records, and track live updates sent from the Smart Kit. The decentralized application (dApp) was built with React, with a focus on functional components, as well as React Hooks such as *useState, useEffect,* and *custom hooks*. Transactions that happen on the chain are handled through Web3.js, with additional metadata drawn from a secure database on the backend for off-chain purposes. With such modular architecture, maintainability, responsive design, and proper rendering speeds are enhanced.

A role-based access control mechanism governs user permissions within the application layer and is enforced directly through the smart contract logic. The system defines distinct roles -such as Manufacturer, Service Provider, Insurance Company, Regulator, and Owner- each associated with a predefined set of lifecycle operations. Authorization is validated on-chain through sender verification, where functions can only be executed if *msg.sender* belongs to the corresponding authorized address list. For example, the recordkeeping of events related to maintenance is restricted to authorized service providers, insurance companies are allowed to provide accident reports, and regulatory bodies are restricted to read-only inquiries. Thus, this permissioned system helps maintain the integrity of events related to the lifecycle that may not be performed by any other unauthenticated user.

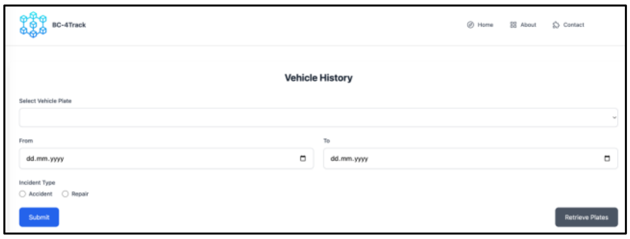
Figure 5 illustrates the primary interface views of the BC-4Track dApp. The main page (Figure 5-a) serves as the central navigating hub for accessing system services. The Owner List interface (Figure 5-b) displays the list of enrolled car owners, allowing authorized persons to create a new record, with every record being immutable and entered into the blockchain after the completion of every transaction. The Vehicle Incident Form interface (Figure 5-c) allows users to enter incident reports, with all entered information being entered into the blockchain. Finally, the Vehicle History interface (Figure 5-d) provides users with the ability to search through previous incident occurrences via the car's license number, combined with the ability to choose a desired date range, allowing users to examine historical events recorded through the system.

(a)

(b)



(c)



(d)

Fig. 5: BC-4Track web application user interface
Source: created by the authors

5 Results and Discussion

The BC-4Track system underwent a series of functional, performance, and reliability tests to validate its operational readiness under realistic usage scenarios. Functional testing confirmed that all smart contract functions -including asset registration, incident recording, and historical data retrieval- executed successfully across multiple stakeholder nodes with a 100% success rate. This uniformity across the nodes verifies that the Solidity-based smart contract logic is indeed right, as well as the robustness of the Remix IDE-supported deployment process.

Usability testing indicated that the system provides intuitive interaction capabilities. An average query processing time for historical information on the blockchain was in the range of 2-3 seconds, while the processing time for events was in the range of 5-7 seconds, depending on the network. These results indicate that the application layer meets the real-time operational requirements of the system, maintaining both responsiveness and reliability under active usage.

As presented in Table 1, performance benchmarking showed that on-chain queries for historical records completed in an average of 2.4 seconds, while new event submissions achieved transaction finality within 6.1 seconds under normal network load. These results place the system's operational speed within the expected range for private Ethereum-based deployments, where block times and consensus latency are typically optimized compared to public networks. For typical vehicle lifecycle tracking scenarios, such as recording accidents or repairs, this latency is sufficiently low to support near real-time decision-making.

Table 1: System Testing Results

Type	Metric	Result
Functional Testing	Smart contract function success rate	100%
Performance (Latency)	Average historical query time	2.4 s
Performance (Finality)	Average new event confirmation	6.1 s
Stress Testing	Max throughput without data inconsistency	~8.3 transactions per minute
Reliability Testing	Unauthorized modification rejection	100%

Source: created by the authors

Stress testing further assessed the system's scalability and throughput. The network maintained stable latency and no data inconsistency at a maximum observed throughput of approximately 8.3 transactions per minute (≈500 tx/hr) without any degradation in consensus performance. While this throughput is more than adequate for low- to medium-frequency event logging (such as fleet tracking or insurance reporting), high-frequency IoT data ingestion (such as continuous telemetry streaming) would require optimization through batching, off-chain aggregation, or Layer-2 scaling solutions.

Although the measured throughput may appear modest compared to high-frequency IoT systems, it is fully adequate for lifecycle events such as ownership changes, maintenance updates, inspections, and accident reports, which occur at low to medium frequency. These operations do not require continuous telemetry, and therefore, the observed 8.3 transactions per minute comfortably support the system's real-time operational needs. Higher-frequency scenarios could be supported in future versions through lightweight Layer-2 extensions or batching techniques.

Reliability testing involved simulating any form of unauthorized changes, all of which were subsequently refused through the network's consensus method. It can be seen that the system can ensure the integrity of the associated data as well as provide tamper-proof capabilities, as expected in its main task of providing a reliable vehicle life cycle ledger.

From the operational standpoint, the results show that BC-4Track meets its design goal for real-time, secure, and auditable vehicle lifecycle management. This is evidenced by the low query time, as well as the finality time, which enables users to effectively engage with the system without any delay that might interfere with their workflow. Furthermore, the zero-failure rate, as well as the consistent rejection of unauthorized modifications, shows that the system is robust.

Although the proposed solution meets the required conditions of the use cases, its throughput may become a concern in production-level deployments, as thousands of vehicles may generate events in parallel. Future studies may focus on addressing scalability issues through the use of hybrid models, such as off-chain storage, sharding, or side chains. Also, incorporating accessibility through mobile devices, as well as interfacing with third-party APIs, may increase the adoption rate.

6 Conclusion

This research demonstrated how blockchain and IoT technologies can be effectively integrated to address long-standing trust, transparency, and data integrity challenges in multi-stakeholder environments. Using the automotive industry as an example, BC-4Track, which is a combination of IoT-based Smart Kits, Ethereum's smart contracts, and a decentralized web application, provides a secure, immutable, and easily accessible system for managing the entire lifecycle of vehicles.

Performance and reliability analyses confirmed that the system was able to record events with low latency as well as resist all forms of unauthorized attempts to modify events. BC-4Track helps remove single points of failure, thus offering significant advantages in terms of minimizing disputes, maximizing regulatory compliance, and increasing efficiency.

Apart from its contributions within the domain, this system presents a generic architectural paradigm that would be applicable in any system requiring synchronized, verifiable, and cross-organization data sharing. Its combination of IoT-driven event acquisition, permissioned blockchain validation, and role-based interaction logic provides a transferable model that can be adapted to contexts such as supply chain tracking, public service registries, and asset management ecosystems.

Although originally developed within the automotive industry, this solution can easily be applied elsewhere in which shared, trusted, and immutable records play a critical task. Future applications will focus on scaling improvements within Layer-2 solutions, off-chain designs, and industry platforms. Other improvements, such as integration with the mobile web or third-party API use, may further enhance its application.

Acknowledgement:
This work is funded by Turkcell Technology A.S. and TUBITAK (The Scientific and Technological Research Council of Turkey) under the 1505 Program, Project no 5220118.

References:

[1] Cappiello, C., Gal, A., Jarke, M., & Rehof, J. (2020). Data Ecosystems: Sovereign data exchange among organizations (Dagstuhl Seminar 19391). Dagstuhl Reports, 9(9), 66-134. doi:10.4230/DagRep.9.9.66

[2] Garcia, R. D., Ramachandran, G. S., Jurdak, R., & Ueyama, J. (2022). Blockchain-aided and privacy-preserving data governance in multi-stakeholder applications. IEEE Transactions on Network and Service Management, 19(4), 3781-3793. doi:10.1109/TNSM.2022.3225254

[3] Helms, M. M., Hervani, A. A., Nandi, S., & Sarkis, J. (2024). A multi-stakeholder digital ecosystem perspective for sustainability and resilience of supply chains. In Environmentally Responsible Supply Chains in an era of digital transformation (pp. 36-57). Edward Elgar

Publishing. doi: 10.4337/9781803920207.00008

[4] Paik, H. Y., Xu, X., Bandara, H. D., Lee, S. U., & Lo, S. K. (2019). Analysis of data management in blockchain-based systems: From architecture to governance. IEEE Access, 7, 186091-186107. doi: 10.1109/ACCESS.2019.2961404

[5] Salman, O., Elhajj, I., Kayssi, A., & Chehab, A. (2015, November). An architecture for the Internet of Things with decentralized data and centralized control. In 2015, IEEE/ACS 12th International Conference of Computer Systems and Applications (AICCSA) (pp. 1-8). IEEE. doi: 10.1109/AICCSA.2015.7507265

[6] Reddy, K. R. K., Gunasekaran, A., Kalpana, P., Sreedharan, V. R., & Kumar, S. A. (2021). Developing a blockchain framework for the automotive supply chain: A systematic review. Computers & Industrial Engineering, 157, 107334. doi: 10.1016/j.cie.2021.107334

[7] Yasin, G., Tyagi, A. K., & Nguyen, T. A. (Eds.). (2024). Blockchain Technology in the Automotive Industry. CRC Press. doi: 10.1201/9781003450306

[8] Jabbar, R., Dhib, E., Said, A. B., Krichen, M., Fetais, N., Zaidan, E., & Barkaoui, K. (2022). Blockchain technology for intelligent transportation systems: A systematic literature review. IEEE Access, 10, 20995-21031. doi: 10.1109/ACCESS.2022.3149958

[9] Kumi, S., Lomotey, R. K., & Deters, R. (2022). A Blockchain-based platform for data management and sharing. Procedia Computer Science, 203, 95-102. doi: 10.1016/j.procs.2022.07.014

[10] Shi, P., Wang, H., Yang, S., Chen, C., & Yang, W. (2021). Blockchain- based trusted data sharing among trusted stakeholders in IoT. Software: practice and experience, 51(10), 2051-2064. doi: 10.1002/spe.2739

[11] Wei, Q., Li, B., Chang, W., Jia, Z., Shen, Z., & Shao, Z. (2022). A survey of blockchain data management systems. ACM Transactions on Embedded Computing Systems (TECS), 21(3), 1-28. doi: 10.1145/3502741

[12] Guo, H., & Yu, X. (2022). A survey on blockchain technology and its security. Blockchain: research and applications, 3(2), 100067. doi: 10.1016/j.bcra.2022.100067

[13] Rajasekaran, A. S., Azees, M., & Al-Turjman, F. (2022). A comprehensive survey on blockchain technology. Sustainable Energy Technologies and Assessments, 52, 102039. doi: 10.1016/j.seta.2022.102039

[14] Coskun, V., Alsadi, M., Kose, B. O., Mantar, H. A., & Oral, M. A. (2023, November). BC-4Track: A Blockchain-based System for Vehicle Tracking Management. In 2023 7th International Symposium on Innovative Approaches in Smart Technologies (ISAS) (pp. 1-5). IEEE. doi: 10.1109/ISAS60782.2023.10391402

[15] Wang, Z. J., Chen, Z. S., Xiao, L., Su, Q., Govindan, K., & Skibniewski, M. J. (2023). Blockchain adoption in sustainable supply chains for Industry 5.0: A multistakeholder perspective. Journal of Innovation & Knowledge, 8(4), 100425. doi: 10.1016/j.jik.2023.100425

[16] Yadlapalli, A., Rahman, S., & Gopal, P. (2022). Blockchain technology implementation challenges in supply chains–evidence from the case studies of multi-stakeholders. The International Journal of Logistics Management, 33(5), 278-305. doi: 10.1108/IJLM-02-2021-0086

[17] Zaabar, B., Cheikhrouhou, O., Jamil, F., Ammi, M., & Abid, M. (2021). HealthBlock: A secure blockchain-based healthcare data management system. Computer Networks, 200, 108500. doi: 10.1016/j.comnet.2021.108500

[18] Attaran, M. (2022). Blockchain technology in healthcare: Challenges and opportunities. International Journal of Healthcare Management, 15(1), 70-83. doi: 10.1080/20479700.2020.1843887

[19] Piccardo, G., Conti, L., & Martino, A. (2024). Blockchain technology and its potential to benefit public services provision: A short survey. Future Internet, 16(8), 290. doi: 10.3390/fi16080290

[20] Shahaab, A., Khan, I. A., Maude, R., Hewage, C., & Wang, Y. (2023). Public service operational efficiency and blockchain–A case study of Companies House, UK. Government Information Quarterly, 40(1), 101759. doi: 10.1016/j.giq.2022.101759

[21] Martinez, D., Magdalena, L., & Savitri, A. N. (2024). AI and blockchain integration: Enhancing security and transparency in financial transactions. International Transactions on Artificial Intelligence, 3(1), 11-20. doi: 10.33050/italic.v3i1.651

[22] Alemany, P., Muñoz, R., Martrat, J., Pastor, A., Díaz, R., Lopez, D., ... & Vilalta, R. (2023). Blockchain-based trust management collaborative system for transport multi-

stakeholder scenarios. Journal of Optical Communications and Networking, 15(8), 488-496. doi: 10.1364/JOCN.486503

[23] Cui, J., Ouyang, F., Ying, Z., Wei, L., & Zhong, H. (2021). Secure and efficient data sharing among vehicles based on a consortium blockchain. IEEE Transactions on Intelligent Transportation Systems, 23(7), 8857-8867. doi: 10.1109/TITS.2021.3086976

[24] Karaduman, Ö., & Gülhas, G. (2025). Blockchain-Enabled Supply Chain Management: A Review of Security, Traceability, and Data Integrity Amid the Evolving Systemic Demand. Applied Sciences (2076-3417), 15(9). doi: 10.3390/app15095168

[25] Kostopoulos, N., Stamatiou, Y. C., Halkiopoulos, C., & Antonopoulou, H. (2025). Blockchain applications in the military domain: A systematic review. Technologies, 13(1), 23. doi: 10.3390/technologies13010023

[26] Wang, X., Zhu, H., Ning, Z., Guo, L., & Zhang, Y. (2023). Blockchain intelligence for the Internet of vehicles: Challenges and solutions. IEEE Communications Surveys & Tutorials, 25(4), 2325-2355. doi: 10.1109/COMST.2023.3305312

[27] Xu, C., Wu, H., Liu, H., Gu, W., Li, Y., & Cao, D. (2022). Blockchain-oriented privacy protection of sensitive data in the Internet of vehicles. IEEE Transactions on Intelligent Vehicles, 8(2), 1057-1067. doi: 10.1109/TIV.2022.3164657

[28] Jain, S., Ahuja, N. J., Srikanth, P., Bhadane, K. V., Nagaiah, B., Kumar, A., & Konstantinou, C. (2021). Blockchain and autonomous vehicles: Recent advances and future directions. IEEE Access, 9, 130264-130328. doi: 10.1109/ACCESS.2021.3113649

[29] Kumar, S., Velliangiri, S., Karthikeyan, P., Kumari, S., Kumar, S., & Khan, M. K. (2024). A survey on the blockchain techniques for the Internet of Vehicles security. Transactions on Emerging Telecommunications Technologies, 35(4), e4317. doi: 10.1002/ett.4317

[30] Gupta, R., Kumari, A., & Tanwar, S. (2021). A taxonomy of blockchain envisioned edge- as-a- connected autonomous vehicles. Transactions on Emerging Telecommunications Technologies, 32(6), e4009. doi: 10.1002/ett.4009

Contribution of Individual Authors to the Creation of a Scientific Article (Ghostwriting Policy)

The authors equally contributed to the present research, at all stages from the formulation of the problem to the final findings and solution.

Sources of Funding for Research Presented in a Scientific Article or Scientific Article Itself

No funding was received for conducting this study.

Conflict of Interest

The authors have no conflicts of interest to declare that are relevant to the content of this article.