International Journal of Safety and Security Engineering
Vol. 16, No. 6, June, 2026, pp. 1279-1286
Journal homepage: http://iieta.org/journals/ijsse

A Blockchain-Based Vehicle Customs Clearance System for Secure Sequential Verification and Fraud Detection

Noor Alhuda Omran Mohammed[1*], Israa Tahseen Ali Al-Attar[1], Faiz A. Al Alawy[2]

[1] Department of Computer Technical Engineering, Technical Engineering College for Computer and AI, Northern Technical University, Kirkuk 36001, Iraq
[2] College of Engineering, Kent State University, Kent OH 44242, USA

Corresponding Author Email: noor_alhuda.omran25@ntu.edu.iq

https://doi.org/10.18280/ijsse.160610

Received: 30 April 2026
Revised: 10 June 2026
Accepted: 17 June 2026
Available online: 30 June 2026

Keywords:
audit trail, blockchain, customs clearance, fraud detection, vehicle verification

ABSTRACT

This paper proposes a blockchain-based vehicle customs clearance system to overcome the limitations of paper-driven processes, including traceability deficiencies and susceptibility to data manipulation. The architecture employs a cryptographically protected hash-chained ledger enforcing a sequential five-stage clearance workflow (ENTRY → INSPECTION → PAYMENT → APPROVAL → EXIT). A rule-based multi-attribute verification mechanism cross-checks seven vehicle attributes against the immutable ENTRY profile at each subsequent stage. The fraud detection logic classifies discrepancies into three severity levels—MEDIUM, HIGH, and CRITICAL—enabling proportionate officer response. Experimental evaluation demonstrates complete detection of all predefined fraud scenarios (21/21, 100%), correct rejection of all invalid stage transitions (15/15), zero identifier collisions across 10,000 generated permit IDs, and an average block insertion latency of 0.82 ms under controlled single-node conditions. The cryptographic design ensures tamper-evidence and transaction authenticity through hash chaining, digital signatures, and Merkle-root verification.

1. INTRODUCTION

Customs authorities worldwide function as critical gatekeepers at national borders, responsible for verifying the identity and legality of vehicles, cargo, and documentation. In many developing nations, this process relies on manual checks, paper records, and disconnected information systems, rendering it inefficient and vulnerable to abuse [1]. Vehicle identity fraud—cloned licence plates, forged chassis records, and falsified engine numbers—poses a growing threat to national security, tax revenue, and public safety [2].

Blockchain technology offers a paradigm for maintaining tamper-evident distributed records without a centralised authority [3]. Properties such as immutability, cryptographic security, and auditability make it well-suited to applications where data integrity is paramount [4].

To the best of the authors' knowledge, prior studies have addressed individual aspects of blockchain-based customs processing, vehicle authentication, fraud detection, or e-government services. However, limited research has integrated sequential workflow enforcement, multi-attribute vehicle verification, severity-classified fraud alerting, and multilingual operational support within a unified customs clearance prototype.

Contributions: C1: Cryptographically protected hash-chained ledger and a sequential 5-step clearance process (ENTRY → INSPECTION → PAYMENT → APPROVAL → EXIT). C2: Cryptographic stage-ordering, to ensure that the execution of the stages is not in violation of or duplicated. C3: Multi-Attribute vehicle verification based on the fixed profile (ENTRY). C4: Fraud detection severity (MEDIUM, HIGH, CRITICAL). C5: Multilingual role based web dashboard (in Arabic and English). C6: Full operational traceability including user identification, terminal identification, alert and correction history and user identification with a comprehensive audit trail.

A single-node blockchain prototype is designed and realized as a cryptographically secure implementation that uses a hash chaining method (SHA-256), digital signatures (Elliptic Curve Digital Signature Algorithm (ECDSA)) and Merkle-root verification and encrypted ledger storage. Distributed consensus and smart-contract functionality are not studied here and will be part of future work.

The paper is structured as follows. Section 2 reviews related literature. Section 3 describes the system architecture, including the web-based dashboard. Section 4 presents the blockchain design and the fraud detection mechanism. Section 5 reports the experimental evaluation. Section 6 discusses the findings. Section 7 concludes.

2. RELATED WORK

2.1 Blockchain in customs and border control

Recent research has shown the potential benefits of blockchain technology in customs operations, vehicle authentication, and fraud prevention. Early customs-oriented blockchain frameworks were discussed in these studies [5, 6], while later studies extended these concepts to operational customs and logistics environments [7, 8]. Several efforts have been proposed for blockchain-based customs solutions to improve data integrity and regulatory compliance in customs processes but most are still in concept and do not support vehicle level authentication or process workflow control. Other solutions have been based on transportation and customs-related solutions, which have adopted the blockchain, IPFS and NFT technologies to secure document management and show the cyber-resilience of the solution, but without implementing multi-attribute vehicle verification or sequential stage control [7, 8]. Additionally, blockchain has been paired with statistical and machine learning methods for customs risk assessment and anomaly detection, and these solutions typically involve a risk score but do not necessarily enforce the workflow deterministically or enforce severity checks for attributes [9, 10]. Thus, the current customs clearance systems do not address the integration of workflow enforcement, multi-vehicle attribute verification, and structured fraud alert [11, 12].

2.2 Blockchain for vehicle identity and registration

Blockchain technology has been used more and more in the vehicle authentication, record management, registration, and certification. Previous works have shown that distributed ledgers could be used to enhance vehicle identity protection, track the origin of a vehicle, record the integrity of the documents involved, and provide security for the vehicle's identity during document verification, including using digital signatures and blockchain-based registration systems [13-19]. The methods presented contribute to the vehicle record management and anti-forgery protection but are mainly concerned with the registration, authentication or record-tracking operation. The existing literature does not fully tackle real-time multi-attribute cross-verification in the midst of customs processing, severity classification of fraud detection and strict enforcement of the sequential processing.

2.3 E-government and fraud detection

In the literature, several permissioned blockchain architectures have been studied for various applications, including government record management, identity management, government document sharing, vehicular network integrity, and smart government applications [20-27]. The studies illustrate how blockchain technology can enhance transparency, auditing, trust and security in public-sector services. Besides, blockchain-based audit trails have been investigated for fraud detection [28] and anomaly classification [29], and immutability of record management has been demonstrated to decrease the opportunities for tax evasion and document fraud. In spite of these developments, current solutions are limited to general e-government services and record management in public-sector workflow, and do not consider the detection of attribute mismatch, enforcement of sequential workflow, or severity-classified fraud alerting in an operational customs clearance workflow.

2.4 Research gap

Table 1 summarises the capabilities of existing approaches relative to the proposed system.

As shown in Table 1, no existing system simultaneously provides end-to-end stage enforcement, multi-attribute vehicle verification, severity-classified fraud alerts, and a role-based multilingual interface. In Table 1, "√" denotes explicit implementation with experimental validation, while "Partial" denotes limited implementation of the capability without full workflow integration, as reported in the cited works. Comparisons are feature-based and derived from published system descriptions rather than direct experimental benchmarking.

Table 1. Comparison of related systems

Reference	Year	Stage Enforcement	Multi-Attribute	Alert Severity	UI	Scope
[5]	2020	×	×	×	×	Conceptual
[7]	2023	Partial	×	×	×	Rail cargo
[8]	2023	×	×	×	×	Documents
[13]	2020	×	Partial	×	×	Registration
[9]	2024	×	×	Partial	×	Risk scoring
[10]	2024	×	×	Partial	×	Risk scoring
This work	2026	√ 5 stages	√ 7 attr.	√ 3 levels	√ AR/EN	Clearance

3. SYSTEM ARCHITECTURE

The proposed system adopts a three-tier layered architecture. The Customs Stages layer enforces the sequential workflow (ENTRY → INSPECTION → PAYMENT → APPROVAL → EXIT). The Blockchain Layer handles cryptographic block creation, hash linking, and immutable ledger storage. Multi-attribute validation and fraud detection operate between these two layers.

The system is a single-node prototype; distributed deployment is identified as future work in Section 7. Rule-based verification was selected over machine learning to ensure transparency and auditability, which are critical requirements in operational customs environments.

Figure 1 illustrates the overall system architecture. The User Tier provides a web dashboard. The Application Tier hosts the blockchain engine, multi-attribute validation, and fraud alert generation. The Persistence Tier maintains the immutable ledger.

3.1 Stakeholders and roles

The four officer classes are audit officers who deal with vehicle registration and record keeping of inspection activities, FEES officers who deal with accounting, valuation and banking, APPROVAL officers who conduct directorial review, notarisation and formal approval, and ISSUANCE officers who issue the final customs permit.

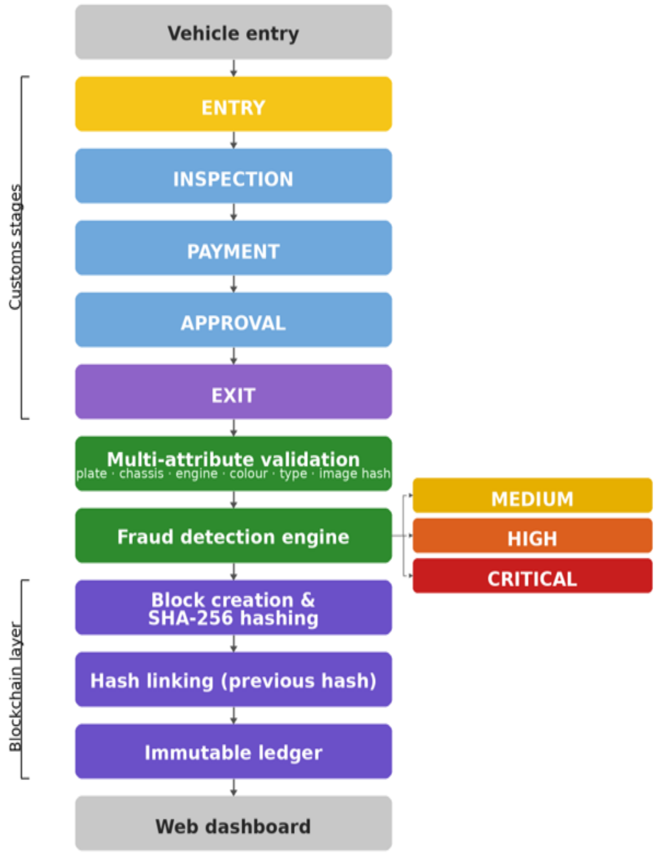

Figure 1. Overall architecture of the proposed blockchain-based vehicle customs clearance system, showing workflow enforcement (ENTRY → EXIT), multi-attribute verification, fraud detection, and blockchain ledger interaction

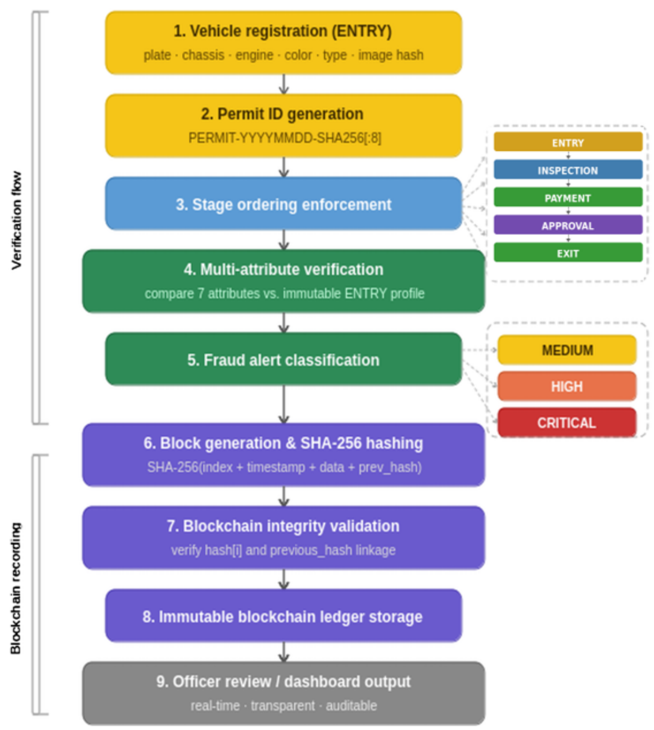

Figure 2. Sequential workflow of the proposed system across five clearance stages, including multi-attribute verification, fraud detection, and blockchain recording at each stage
Note: Director review and other administrative checks are sub-processes within the APPROVAL stage and are not treated as independent blockchain workflow stages.

3.2 Data flow

As illustrated in Figure 2, the vehicle is registered by an audit officer at the ENTRY stage, where the plate number, chassis number, engine number, vehicle color, vehicle type, and SHA-256 image hash are recorded. An ENTRY block is then created and appended to the ledger, and the system automatically generates a permit identifier. The workflow subsequently progresses through the INSPECTION, PAYMENT, APPROVAL, and EXIT stages. At each stage, all seven attributes are cross-verified against the immutable ENTRY profile, and severity-classified alerts are generated whenever discrepancies are detected. Upon successful completion of all workflow stages, the vehicle is authorized to leave.

3.3 Web-based dashboard

The Customs Gateway Web Dashboard is a single-page application (SPA) using JavaScript, HTML5, CSS3. The dashboard is designed to be role-based access control (RBAC) where each officer can only access and participate in certain workflow stages and functions. The Arabic RTL interface has been developed to assist customs officers from beginning to end in their administrative process, following the RBAC principles of blockchain-based e-government systems [20]. The twelve administrative workflow steps and the five technical blockchain stages are mapped in Table 2, which clarifies the mapping ambiguity from the workflow mapping identified in the review.

Table 2. Administrative-to-blockchain stage mapping

Step	Administrative Stage	Blockchain Stage	Officer Role
1	Incoming	ENTRY	AUDIT
2	Inspection	INSPECTION	AUDIT
3	Print Letter	INSPECTION	AUDIT
4	Specialist Review	INSPECTION	AUDIT
5	Audit	INSPECTION	AUDIT
6	Accounting	PAYMENT	FEES
7	Valuation	PAYMENT	FEES
8	Bank	PAYMENT	FEES
9	Director Review	APPROVAL	APPROVAL
10	Notary	APPROVAL	APPROVAL
11	Director Signature	APPROVAL	APPROVAL
12	Book Receipt	EXIT	ISSUANCE

Cases progress through five states: PENDING, IN_REVIEW, APPROVED, REJECTED, and DONE. Vehicle images are base64-encoded and authenticated against the SHA-256 image hash stored in the ENTRY block.

4. BLOCKCHAIN DESIGN AND IMPLEMENTATION

4.1 Block structure

As illustrated in Figure 3, each block contains eight fields: index, timestamp (ISO-8601 UTC), vehicle_id, stage, permit_id, data (stage-specific vehicle attributes), previous_hash (SHA-256 of the preceding block), and hash (SHA-256 of current block contents). The block hash is computed as:

$$\text{hash}(B_i) = \text{SHA-256}(\text{JSON}^N(\{\text{index, timestamp, vehicle\_id, stage, permit\_id, data, previous\_hash, created\_by}\}))$$

where, JSON^N applies lexicographic key sorting and UTF-8 encoding for deterministic serialisation [30]. Modification of any block B_i invalidates the hashes of all subsequent blocks, providing comprehensive tamper detection [4].

In addition to SHA-256 hash chaining, each block is digitally signed using the ECDSA-SHA256. Public–private key pairs are assigned to authorised participants, and signature verification is performed during chain validation to ensure transaction authenticity, integrity, and non-repudiation. Furthermore, a Merkle root is computed from the block contents to strengthen integrity verification and facilitate tamper detection. This design constitutes a cryptographically secured hash-chained prototype rather than a distributed blockchain with consensus. The security guarantee provided is tamper-evidence through hash linkage, not Byzantine fault tolerance. Distributed deployment is a defined direction for future work. Blockchain records are stored in encrypted form using symmetric encryption, providing an additional confidentiality layer for persisted vehicle records.

4.2 Genesis block and permit ID generation

The ledger initialises with a genesis block assigned vehicle_id = 'GENESIS' and previous_hash = '0' [3]. Upon ENTRY registration, a permit identifier is generated as: permit_id = 'PERMIT-{YYYYMMDD}-' + SHA-256('PERMIT|{vehicle_id}|{UTC_timestamp}|{chain_length}') [8]. Zero collisions were observed across 10,000 generated identifiers.

4.3 Stage ordering and chain integrity

Stage ordering is enforced through three constraints: (1) the initial constraint requires that every vehicle's first recorded stage is ENTRY; (2) the uniqueness constraint prohibits any stage from being recorded more than once per vehicle; (3) the ordering constraint ensures that all stages follow the prescribed sequence without omission or bypass. The validate_chain() method performs an O(n) full-chain audit, verifying both hash correctness and previous_hash linkage [4]. Chain validation includes verification of block hashes, previous-hash linkage, and digital signatures. Any modification to signed block contents invalidates the corresponding signature and is detected during validation.

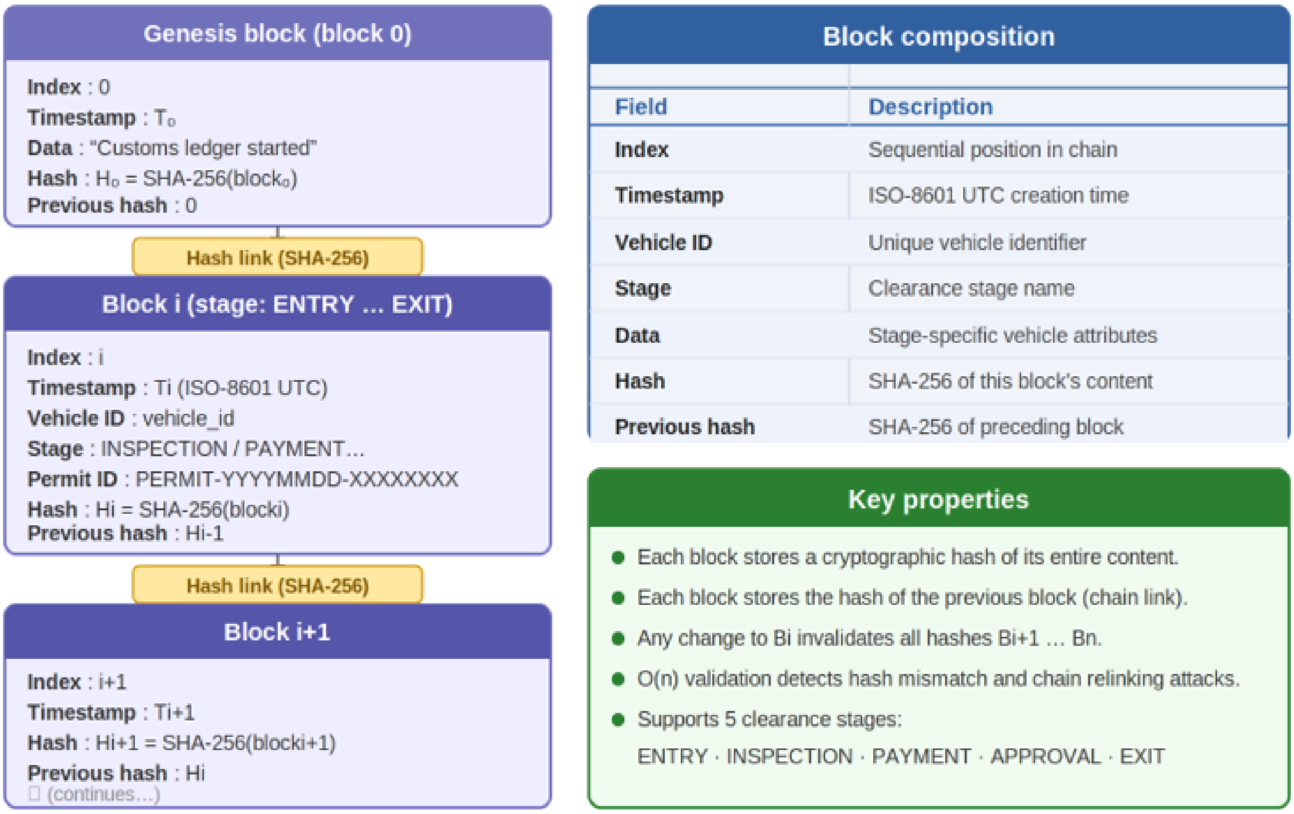

Figure 3. Blockchain block structure of the proposed system, showing index, timestamp, data, hash, and previous_hash fields ensuring tamper-evident integrity through SHA-256 hash linkage

4.4 Fraud detection mechanism

Vehicle profile and alert classification

The ENTRY block is the reference block that cannot be modified. Each of the following stages involves a cross-verification of 7 attributes: permit_id, plate_number, chassis_number, engine_number, car_colour, car_type and image_hash (SHA-256 of the image of the car taken at ENTRY). Table 3 provides details of the types and severity of alerts.

Alert record structure

Alerts are recorded as structured dictionaries containing vehicle_id, alert_type, severity, message, stage, and timestamp. Alerts are non-blocking by design: they are logged to the audit trail without interrupting blockchain recording, preserving forensic completeness regardless of officer action [9]. Officers may override alerts in exceptional circumstances, with all overrides permanently logged.

Table 3. Alert types and severity classification

Alert Type	Attribute	Severity	Rationale
PERMIT_MISMATCH	permit_id	HIGH	Permit document inconsistency
PLATE_MISMATCH	plate_number	HIGH	Licence plate substitution
CHASSIS_MISMATCH	chassis_number	CRITICAL	Vehicle identity fraud (VIN cloning)
ENGINE_MISMATCH	engine_number	CRITICAL	Engine substitution
COLOR_MISMATCH	car_colour	MEDIUM	Vehicle repainting or misrepresentation
TYPE_MISMATCH	car_type	MEDIUM	Vehicle classification inconsistency
IMAGE_HASH_MISMATCH	image_hash	HIGH	Image manipulation or vehicle substitution

Note: CRITICAL alerts (chassis and engine mismatches) carry the highest risk as these identifiers are legally definitive for vehicle identity [1]. HIGH alerts indicate strong evidence of document or physical fraud [28]. MEDIUM alerts trigger investigative review without mandatory vehicle detention.

5. EXPERIMENTAL EVALUATION

5.1 Experimental setup

The system was implemented in Python 3.10 using standard library modules (hashlib, json, datetime) on a single workstation (Intel Core i7, 16 GB RAM, Ubuntu 22.04). All experiments were conducted in a controlled, single-node environment without distributed communication, network latency, or concurrent users. Results characterise the algorithmic performance of the prototype and should not be interpreted as predicting the performance of a deployed distributed system.

The evaluation dataset was derived from 40 anonymized customs-clearance transactions obtained from routine Iraqi customs procedures. Prior to analysis, all personally identifiable and operationally sensitive information was anonymized. Personal names, vehicle-owner information, document reference numbers, official correspondence identifiers, officer names, signatures, and other identifying fields were removed or replaced with pseudonymous identifiers. The resulting records retained only the workflow and verification attributes required for system evaluation. Based on these anonymized records, 21 controlled fraud scenarios covering the seven alert categories presented in Table 3 were constructed to evaluate fraud-detection capabilities. Additionally, 15 invalid workflow-transition scenarios were intentionally created to assess stage-ordering enforcement. No personally identifiable information was retained in the evaluation dataset.

5.2 Chain integrity and stage ordering

A test ledger was built, consisting of 1 genesis + 6 vehicles × 5 stages + 19 other administrative blocks. Earlier, there were four scenarios of tampering evaluated: T1 - Changing chassis_number, T2 - Changing previous_hash, T3 - Duplicating an ENTRY, T4 - Changing plate_number. The detection of T1, T2 and T4 was achieved through the return value of validate_chain(), and the prevention of T3 was done by the stage-ordering logic at insertion. Fifteen invalid stage transitions were all correctly rejected.

5.3 Fraud detection and performance

Table 4 reports detection results for all seven alert types, with three test cases per alert type.

Block insertion latency was measured over 1,000 sequential insertions: average 0.82 ms; full chain validation (1,000 blocks) = 12.4 ms; permit ID generation < 0.1 ms; alert generation < 0.05 ms per attribute check. These figures reflect in-process Python execution without network, consensus, database persistence, or concurrent user overhead.

Table 4. Fraud alert detection results

Alert Type	Severity	Cases	Det.	Rate
CHASSIS_MISMATCH	CRITICAL	3	3	100%
ENGINE_MISMATCH	CRITICAL	3	3	100%
PERMIT_MISMATCH	HIGH	3	3	100%
PLATE_MISMATCH	HIGH	3	3	100%
IMAGE_HASH_MISMATCH	HIGH	3	3	100%
COLOR_MISMATCH	MEDIUM	3	3	100%
TYPE_MISMATCH	MEDIUM	3	3	100%
Total	—	21	21	100%

Table 5. Feature-level comparison with related approaches

Method	Tamper-Proof	Latency (ms)	Stage Enf.	Attr. Verif.
Centralised DB	×	<1 (local)	×	1-2 attributes
[7]	√	N/R¹	Partial	Rail cargo only
[10]	√	N/R¹	×	ML anomaly score
[9]	√	N/R¹	×	Value anomaly
This work	√	0.82, (singl-node)	5 stages	7 attr., 3-level

Note: ¹ N/R = Not Reported: latency data not available in the original publication.
Stage Enf. – programmatic enforcement of workflow ordering. Attr. Verif. refers to the main verification method mentioned for each system. Partial means that the capability is applied, but not included in the entire workflow. Comparisons are made in a feature-based manner and are based on system descriptions published rather than on actual experimental benchmarking.

The reported average block-insertion latency of 0.82 ms indicates that the cryptographic mechanisms incorporated in the proposed prototype, including SHA-256 hash chaining, ECDSA digital signatures, and integrity-validation procedures, introduce only limited computational overhead under the evaluated conditions. However, this measurement was obtained in a controlled single-node environment and reflects the execution cost of the prototype logic itself. It does not include network communication delays, distributed consensus operations, inter-node synchronization, database persistence overhead, or concurrent-user workloads. Therefore, the reported latency should be interpreted as a prototype-level performance indicator rather than a prediction of performance in a production-scale distributed blockchain deployment.

Table 5 provides a feature-level comparison derived from published system descriptions; direct performance benchmarking against the compared systems is not feasible as no shared evaluation benchmark or publicly available implementation exists for the compared approaches.

6. DISCUSSION

The experimental results show that the prototype can meet the design goal under the single-node scope. The rule-based verification and stage-ordering mechanisms identified all predefined fraud patterns across the seven evaluated attributes and prevented all tested invalid workflow transitions. These results prove the correctness of the prototype in the specified test cases.

The rule-based method was intentionally used rather than machine learning methods to give interpretable and auditable decision logic that is appropriate for regulatory environments where officers are required to explain automated alerts [10]. The current scope of detection is for exact-match verification of seven attributes and does not consider partial attribute matches, noisy input data, human transcription errors, or coordinated multi-stage manipulation of the data, or forged images that recreate a legitimate hash. These limitations represent opportunities for future improvement and further investigation. Further, input validation detection is done before the recording on the blockchain, such as the mandatory fields and the consistency of the input formats, and the detection of the missing records does not fall in the range of the automatic detection system which is in place at the moment.

The implementation is a single-node prototype with cryptographic security that uses hash chaining, digital signatures and Merkle-root verification, not Byzantine fault tolerance, to provide tamper-evidence. The 0.82 ms latency is the time for executing an in-process Python script, excluding the time for network or consensus. Future studies will need to understand the scaling behaviour under distributed deployment conditions.

Table 5: Stage Enf. = Programmatic Prevention of Out-of-Order Stage Execution; Attr. Verif. = Cross-Checking of Multiple Vehicle Identity Attributes Against a Fixed Reference Profile. Used as recommended by published descriptions.

Limitations: The evaluation data was based on anonymous data and operational processes from real Iraqi customs workflows. Even though the experimental scale was small, the test scenarios were arranged in such a manner that it was representative of realistic customs processing situations. There are three main limitations of the study. The first is that evaluation was done on a prototype scale, using anonymised customs operational records and customs procedures from Iraq. Although the evaluation was conducted on a prototype scale, the experiments were derived from real operational customs records and procedures. The second is that the prototype is based on a single node and is therefore not distributed consensus or Byzantine fault tolerant. But there are mechanisms for integrity protection including cryptographic hash chaining, digital signatures, merkle-root verification and chain validation. Third, current fraud detection relies on exact-match verification of pre-defined vehicle attributes, while more complex scenarios such as partial-match verification, noisy data, image forgery and large-scale operational validation are further research tasks.

7. CONCLUSION AND FUTURE WORK

This paper presented a blockchain-based vehicle customs clearance prototype enforcing a mandatory five-stage sequential workflow through a hash-chained ledger, with rule-based multi-attribute verification against an immutable ENTRY profile and severity-classified fraud detection. Experimental evaluation confirmed complete detection of all predefined fraud scenarios (21/21), correct rejection of all invalid stage transitions (15/15), zero identifier collisions across 10,000 permit IDs, and an average block insertion latency of 0.82 ms under single-node conditions.

Future work will focus on distributed deployment environments, advanced fraud detection scenarios, and large-scale operational validation using expanded customs datasets.

ACKNOWLEDGMENT

The authors thank the domain experts and supporting institutions whose insights contributed to the design and evaluation of the proposed system.

REFERENCES

[1] Mamyrova, S., Alibayeva, G., Adilova, K., Kussainova, A., Tynybekov, S. (2025). Comparative analysis of digital technologies and legal frameworks in customs operations: A focus on violation detection. Journal of Transportation Security, 18(1): 1-23. https://doi.org/10.1007/s12198-025-00316-9

[2] Leka, E., Lamani, L., Hamzallari, K. (2023). A framework solution for vehicle theft detection by integrating NFC with a blockchain-based system. TEM Journal, 12(4). https://doi.org/10.18421/tem124-16

[3] Ali, O., Jaradat, A., Kulakli, A. (2021). A comparative study: Blockchain technology utilization benefits, challenges and functionalities. IEEE Access, 9: 12730-12749. https://doi.org/10.1109/ACCESS.2021.3050241

[4] Chen, Z., Celik, S.E., Sarkis, J. (2026). A systematic review of academic literature for blockchain application in government and public service. Journal of Enterprise Information Management, 39(1): 381-409. https://doi.org/10.1108/jeim-03-2024-0150

[5] Yaren, H. (2020). Implementing blockchain technology

in the customs environment to support the SAFE Framework of Standards. World Customs Journal, 14(1): 127-138. https://doi.org/10.55596/001c.116314
[6] Elkoutour, M., Raji, H., Bakhat, M. (2024). Blockchain technology and customs clearance procedures: Facilitating and smoothing products importation in Morocco's customs and excises administration. In Sustainable and Green Technologies for Water and Environmental Management, pp. 53-69. https://doi.org/10.1007/978-3-031-52419-6_6
[7] Kim, S., Kim, D. (2023). Securing the cyber resilience of a blockchain-based railroad non-stop customs clearance system. Sensors, 23(6): 2914. https://doi.org/10.3390/s23062914
[8] Rehal, M., Ahuja, R., Gandhi, D., Sharma, A. (2023). A blockchain-based custom clearance solution for international trade using IPFS and non-fungible tokens. In International Conference on Data Analytics & Management, pp. 551-564. https://doi.org/10.1007/978-981-99-6550-2_42
[9] Santos, D.R.D. (2024). Enhancing international trade security: Real-time risk assessment in brazilian customs with blockchain technology. International Journal of Business and Management, 19(6): 49. https://doi.org/10.5539/ijbm.v19n6p49
[10] Shafin, K.M., Reno, S. (2024). A blockchain and machine learning-based integrated framework for dynamic customs security enhancement with a focus on smuggling. In 2024 6th International Conference on Electrical Engineering and Information & Communication Technology (ICEEICT), Dhaka, Bangladesh, pp. 511-516. https://doi.org/10.1109/iceeict62016.2024.10534558
[11] Han, C., Wang, B., Wu, Y., Shi, X. (2024). Research on the construction of cross-border e-commerce Guangdong-Hong Kong full-chain intelligent customs clearance information system. In Proceedings of the 2024 3rd International Conference on Cyber Security, Artificial Intelligence and Digital Economy, Nanjing, China, pp. 188-196. https://doi.org/10.1145/3672919.3672956
[12] Taufiq, R., Warnars, H.L.H.S., Soeparno, H., Oktavia, T., Muyeba, M. (2025). Enhancing traceability in organic rice supply chain with blockchain technology developed by design science research methodology. Organic Farming, 11(4): 277-289. https://doi.org/10.56578/of110404
[13] Das, M., Azad, R.U., Efat, M.I.A. (2020). Blockchain aided vehicle certification (BVC): A secured e-governance framework for transport stakeholders. In 2020 23rd International Conference on Computer and Information Technology (ICCIT), DHAKA, Bangladesh, pp. 1-6. https://doi.org/10.1109/ICCIT51783.2020.9392725
[14] Hossain, M.P., Khaled, M., Saju, S.A., Roy, S., Biswas, M., Rahaman, M.A. (2020). Vehicle registration and information management using blockchain based distributed ledger from Bangladesh perspective. In 2020 IEEE Region 10 Symposium (TENSYMP), Dhaka, Bangladesh, pp. 900-903. https://doi.org/10.1109/TENSYMP50017.2020.9230781
[15] Joseph, M.P., Kukatlapalli, P.K., Shaker, H., Vijaya, P., Jimmy, N. (2023). Smart and secure blockchain structure to track vehicle record-keeping in the sultanate of Oman. International Journal on Recent and Innovation Trends in Computing and Communication, 11(9): 1999-2006. https://doi.org/10.17762/ijritcc.v11i9.9197
[16] Ali, G., ElAffendi, M., Ahmad, N. (2023). BlockAuth: A blockchain-based framework for secure vehicle authentication and authorization. Plos One, 18(9): e0291596. https://doi.org/10.1371/journal.pone.0291596
[17] Chughtai, Z.A., Janjua, J.I. (2025). Block chain enabled vehicle documents verification system. In 2025 International Conference on Metaverse and Current Trends in Computing (ICMCTC), Subang Jaya, Malaysia, pp. 1-7. https://doi.org/10.1109/icmctc62214.2025.11196169
[18] Joseph, M., Shaker, H., Al Hosni, N. (2023). Development of a blockchain-based vehicle history system. In International Conference on Computational Sciences and Sustainable Technologies, pp. 54-65. https://doi.org/10.1007/978-3-031-50993-3_5
[19] Geetha, S., Ashna, P.S., Bhat, A., Singh, H.P. (2024). Vehicular networks: Revolutionizing motor vehicle operations and governance through blockchain. In 2024 International Conference on Advances in Computing, Communication and Applied Informatics (ACCAI), Chennai, India, pp. 1-6. https://doi.org/10.1109/accai61061.2024.10602247
[20] Elisa, N., Yang, L., Chao, F., Cao, Y. (2023). A framework of blockchain-based secure and privacy-preserving e-government system. Wireless Networks, 29(3): 1005-1015. https://doi.org/10.1007/S11276-018-1883-0
[21] Sen, S., Mukhopadhyay, S., Karforma, S. (2021). A blockchain based framework for property registration system in e-governance. International Journal of Information Engineering and Electronic Business, 11(4): 30. https://doi.org/10.5815/IJIEEB.2021.04.03
[22] Chen, J., Li, T., Zhu, R. (2022). Analysis of malicious node identification algorithm of internet of vehicles under blockchain technology: A case study of intelligent technology in automotive engineering. Applied Sciences, 12(16): 8362. https://doi.org/10.3390/app12168362
[23] Ghani, R.F., Al-Karkhi, A.A.S., Mahdi, S.M. (2022). Proposed framework for official document sharing and verification in e-government environment based on blockchain technology. Baghdad Science Journal, 19(6): 45. https://doi.org/10.21123/bsj.2022.7513
[24] Stoica, M., Mircea, M. (2025). Blockchain and Internet of things (BIoT) in smart government-impact analysis. IEEE Access, 13: 144195-144214. https://doi.org/10.1109/access.2025.3599108
[25] Sung, C.S., Park, J.Y. (2021). Understanding of blockchain-based identity management system adoption in the public sector. Journal of Enterprise Information Management, 34(5): 1481-1505. https://doi.org/10.1108/JEIM-12-2020-0532
[26] Sharma, S.K., Pushkar, A., Kumar, A. (2023). The Application of blockchain technology in e-government: Enhancing trust, security and transparency. Zenodo. https://doi.org/10.5281/zenodo.8214610
[27] Abbas, H., Ibrahim, I.E., Esmaiel, H., Abd-El-Atty, B. (2025). Critical infrastructures challenges and requirements meet blockchain features and benefits: A literature review. International Journal of Critical Infrastructures, 21(6): 592-639. https://doi.org/10.1504/IJCIS.2025.150793

[28] Kumar, G., Yamuna, B. (2025). Blockchain-based fraud detection and prevention system enhanced with AI. International Journal for Research in Applied Science and Engineering Technology, 13(9): 538-544. https://doi.org/10.22214/ijraset.2025.73998

[29] Ariyibi, K.O., Bello, O.F., Adediran, O.F., Phillips, A.P., Odumuwagun, O.O., Kazeem, O. (2024). The application of blockchain technology to improve tax compliance and Ensure transparency in global transactions. International Journal of Science and Research Archive, 13(2): 1516-1527. https://doi.org/10.30574/ijsra.2024.13.2.2286

[30] Zhang, Z., Sun, Y., Huang, P., Wang, C. (2022). A blockchain and multi factor fusion based electronic identity registration and verification system. In 2022 3rd International Conference on Computer Science and Management Technology (ICCSMT), Shanghai, China, pp. 431-435. https://doi.org/10.1109/iccsmt58129.2022.00097