OPEN ACCESS Freely available online

International Journal of Advancements in Technology

ISSN: 0976-4860

Research Article

Vehicle Supply Chain Recall Management and Fraud Prevention Using Block Chain

Rukevwe Emmanuel Anaka[*]

Department of Computing and Informatics, Bournemouth University, Poole, United Kingdom

ABSTRACT

The automobile industry is undergoing technological advancement, which includes breakthroughs such as hybrid cars, Electric Vehicles (EVs) and self-driving capabilities. However, despite these advances, issues remain, notably in recall management efficiency, security and risk of fraud. To solve these difficulties, the idea of industry 4.0 has been adopted, which uses technologies such as sensors, IOT's and machine learning. Even this technology still has loopholes in the area of security which has been exploited negatively over time. In other to mitigate these loopholes we introduce block chain technology as a viable alternative, providing a safe and transparent environment. This study investigates and proposed the use of block chain to create an enhanced Vehicle Tracking System (VTS) intended at enhancing recall management and reducing fraud in the automobile sector. The proposed solution was discussed in detail and a mock smart contract was also written, which was deployed on the Ethereum Virtual Machine (EVM).

Keywords: Ethereum Virtual Machine (EVM); Vehicle Tracking System (VTS); Automobile industry; Self-driving capabilities

INTRODUCTION

The automotive industry is a technologically induced field that focuses on making cars and other vehicles. It is a very advanced industry that uses technology to create new and innovative automobiles. Some examples of these innovations are hybrid cars that use both electricity and gasoline, electric cars that run entirely on electricity and self-driving cars that can drive themselves without a human driver, this also brought about the Industrial Internet of Things (IIOT) revolution, in a beat to make cars have internet accessibility connecting with other device such as smart phones. One of the major problems that come with this revolution is the problem of efficiency and security and trust. In other to mitigate this challenge the industry 4.0 concept was adopted, which involve using technology to make things better, such as using things like sensors to collect data, using big data techniques to analyze the data and using new machine learning approaches to make cars smarter. It also includes using new computing methods, like cloud computing, to store and process all the data [1].

Block chain technology can be used to create a safe monitoring system for automobiles, which automakers can use to handle vehicle recalls and stop fraud. Block chain offers a trustworthy, transparent and decentralized ecosystem. It functions more like a large group chat where all participants can view and confirm each other's messages, akin to a unique network that links individual machines. Because information supplied to this network cannot be removed or altered, it is incredibly secure. Numerous industries, including supply chain management, cross-border payments, smart appliances, healthcare management, Internet of Things (IoT) applications and Internet of Vehicles (IoV) have effectively adopted it. Vehicle security may be improved by using block chain, giving users a reliable and safe method they.

This research paper explores the innovative application of block chain technology to address these issues, creating an advanced Vehicle Tracking System (VTS) designed to improve recall management and prevent fraud. The proposed system employs block chain's capabilities to enhance traceability, transparency and data security, thereby significantly enhancing consumer safety.

Correspondence to: Rukevwe Emmanuel Anaka, Department of Computing and Informatics, Bournemouth University, Poole, United Kingdom; E-mail: S5550272@bournemouth.ac.uk

Received: 12-Feb-2024, Manuscript No. ijoat-24-29569; **Editor assigned:** 15-Feb-2024, PreQC No. ijoat-24-29569 (PQ); **Reviewed:** 29-Feb-2024, QC No. ijoat-24-29569; **Revised:** 13-Mar-2025, Manuscript No. ijoat-24-29569 (R); **Published:** 20-Mar-2025, DOI: 10.35841/0976-4860.25.16.345

Citation: Anaka RE (2025) Vehicle Supply Chain Recall Management and Fraud Prevention Using Block Chain. Int J Adv Technol. 16:345.

Problem statement

The traditional approach to vehicle recall management is plagued by inefficiencies and vulnerabilities, leading to prolonged response times and heightened risks for consumers. The lack of transparency in these processes undermines trust in both manufacturers and regulatory bodies. The industry faces rampant fraudulent activities, including the circulation of counterfeit parts, manipulation of vehicle data and the resale of stolen vehicles. Conventional tracking systems are not only prone to data tampering but also fall short in verifying the authenticity of vehicle histories and components. Moreover, the increase in global vehicle theft has lead to the development of several anti-theft systems yet these solutions relying on technologies like IoT, GPS/GSM and biometric identification with data privacy issues and are prone to cybercrime, compromising overall vehicle security.

Block chain technology emerges as a promising solution to these challenges. Its characteristics of decentralization, immutability and transparency can help improve vehicle tracking and recall processes. Block chain's ability to create a tamper-proof ledger ensures reliable and authentic vehicle data, mitigating risks of fraud and theft. Furthermore, the integration of smart contracts can automate recall processes, significantly reducing response time and enhancing consumer safety [2].

MATERIALS AND METHODS

Project objective

- Review existing problem with vehicle traceability and recall.
- Propose a solution to solve the identified problem with vehicle recall.
- Develop a mock implementation to enhance technical guild for development of the proposed solution.

State of art and related works

This section provides state of the act background of the solution and also discuss relevant related state of the art works that has previously been done and proposed.

Vehicle tracking system that uses block chain technology can be an effective way to prevent fraud and recall issues. Block chain is a decentralized and secure platform that can store data immutably and authenticate users automatically with greater accuracy. The immutability, transparency and decentralization nature make it the idea perfect solution to the security challenge in managing vehicle recall. A few existing vehicle anti-theft systems suffer from major problems such as the leakage of personal information, centralized-based system, proper key management and data security (Figure 1).

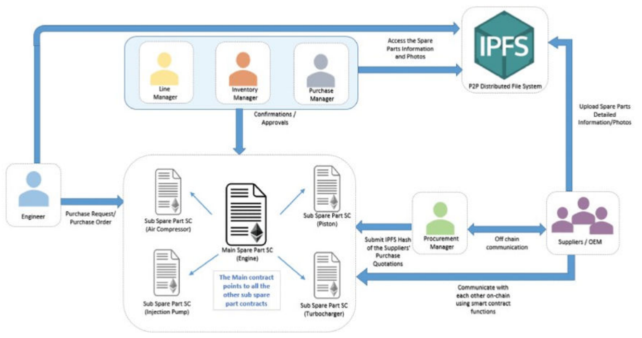

IPFS
P2P Distributed File System
Access the Spare Parts Information and Photos
Line Manager
Inventory Manager
Purchase Manager
Confirmations / Approvals
Upload Spare Parts Detailed Information/Photos
Engineer
Purchase Request/ Purchase Order
Sub Spare Part SC (Air Compressor)
Sub Spare Part SC (Piston)
Main Spare Part SC (Engine)
The Main contract points to all the other sub spare part contracts
Sub Spare Part SC (Injection Pump)
Sub Spare Part SC (Turbocharger)
Submit IPFS Hash of the Suppliers' Purchase Quotations
Procurement Manager
Off chain communication
Suppliers / OEM
Communicate with each other on-chain using smart contract functions

Figure 1: Block diagram of the state of art for an automobile spare part with block chain.

The demand for high-spec vehicles has made the automotive supply chain complex. Automakers use supply chain strategies to improve operations. The automotive supply chain includes both forward and reverse supply chains. Forward supply chain involves stakeholders like parts suppliers, automakers, dealers and consumers. Reverse supply chain starts with product and information flow from consumers to automakers. Product recall is a critical aspect of the reverse supply chain. A product recall is when a manufacturer retrieves faulty goods used by consumers to fix the problems. Vehicle recalls have seen significant increased over 100% per incident between 2016-2017 in the US. These defects pose a significant risk of injury or death and can cause sudden and catastrophic component failures without warning. A study surveyed defects in various automotive systems, including electronics, steering and fuel systems, on 345 passenger vehicles in the U.S. It found that half of all recalls were related to vital automotive components and systems.

Block chain technology proposed for recalling vehicles focuses on eliminating the sale of counterfeit auto parts, ensuring safety for consumers and reducing delays for automakers. Benatia offers a big data-driven framework for food product traceability, aiming to improve tracking and lower recall costs. This system involves multiple stakeholders, including manufacturers and customers. The prof of work consensus protocol used does not really make room for easy scalability and also centralized data storage which makes it easy for attack and compromise. It uses big data to manage vast data volumes, gathering product information like ID, condition and location *via* mobile apps and QR-Code technology. However, it doesn't specifically tackle the problem of product counterfeiting, a key issue in recalls [3].

Figure 2 demonstrates the initial effort to gather data for progressive tracking involved using an On-Board Diagnostics (OBD) device to collect Diagnostic Trouble Codes (DTCs) and transmit them to a server *via* WiFi. However, this method has significant security flaws due to the absence of encryption, making the data vulnerable. Moreover, the necessity to collect data at specific times on a single server introduces the risk of a single point of failure.

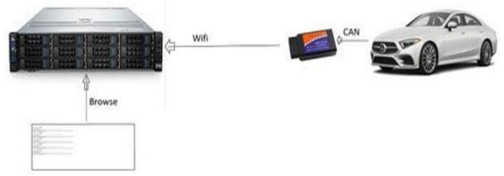


Figure 2: OBD and Wi-Fi data collection.

Block chain technology was integrated by Shafii as a more complex method to enhance the process. This technology was utilized to maintain a database for recording the histories and service maintenance of vehicles in the system. This system enabled various stakeholders, including vehicle owners, maintenance workshops, dealers and insurance companies, to add blocks to the block chain, ensuring continuous monitoring of the vehicle's history and services. Each aspect of the vehicle's life cycle was to be manually documented, building a comprehensive history chain. However, a significant limitation of this approach was the need for manual data collection and verification by the insurance company connected.

Yoo and Ahn identified issues related to data leakage as outlined in. The system highlighted the recall process and the reporting mechanism to the automakers. A significant problem in this process is the heavy reliance on end-users for detection and reporting, leading to diminished trust in the brand. This recall process is illustrated in Figure 3.

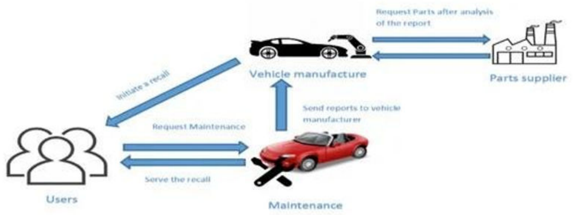


Figure 3: Manual reported recall process.

Also, Sharma proposed a different architecture illustrated in Figure 4 using a block chain architecture in smart cities for data collection and block chain uploading. However, this approach encounters the same challenge of manual data entry, affecting the data's reliability.

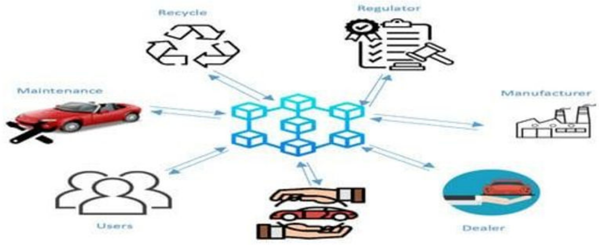


Figure 4: Distributed block chain system for smart city automobile.

Proposed solution

This research majorly provide solution for the security challenge in the vehicle recall management and fraud prevention. We are leveraging on block chain's immutability, transparency and decentralization nature. Data integrity is paramount as immutability ensures that vehicle data, such as location, mileage and maintenance history is reliably stored accessed only by authorized stakeholder in the chain. This reliability is crucial for accurate tracking and assessment of vehicle conditions. In this proposal we've eliminated the manual upload of data by participant in the system and therefore introduce automated IOT data collection [4].

When a recall is reported, manufacturers need accurate and tamper-proof vehicle histories to identify affected models and parts. Block chain's immutability guarantees the authenticity of this data, aiding in precise recall targeting and reducing the risk of overlooking defective vehicles or including unaffected ones. The system is designed to build trust and transparency among users. Vehicle owners can access their vehicle data, ensuring openness in how their data is used and managed. The transparency aids in maintaining regulatory compliance and public trust. Regulatory bodies and auto-owners can independently verify the accuracy of recall-related information, leading to increased confidence in the recall process and the manufacturer's commitment to safety.

The Proof of Work (PoW) and Byzantine Fault Tolerance (BFT) consensus mechanisms is used to achieve decentralization in the proposed system where multiple nodes validate and confirm transactions. Datas are not stored in a centralized server rather across a network of nodes, making it resistant to cyber-attacks and data breaches. The decentralized nature of the system ensures it resilience against tampering and fraud, as altering recall data would require consensus across the majority of nodes, which is impractical and highly unlikely.

In other to secure data access in the proposed system we intend implement smart contract using solidity in Ethereum Virtual Machine (EVM), a high-level language designed for implementing smart contracts on various block chain platforms. These contracts are executed on the EVM, an isolated environment ensuring security and integrity. The smart contract component would include.

Data structures: This will be used to store vehicle data, such as vehicle identity, location data, maintenance records and recall status.

Functions: To handle various operations like data entry, validation and retrieving of data. These include functions for adding new vehicle data, validating data authenticity and providing access control.

Modifiers: These will be used for access control, ensuring only authorized entities (like manufacturers, dealers or regulatory bodies) can input or modify data.

Validation logic: Incorporates logic to validate the integrity and authenticity of the data received from IoT devices.

IoT devices in vehicles collect data (e.g., location, speed, engine status and performance). This data is transmitted securely (using cryptographic encryption and secure channels) to the block chain network. Smart contracts receive this data and perform necessary validations before storing it on the block chain [5].

When data retrieval is requested, smart contracts validate the identity and authorization of the requester. For fraud prevention, smart contracts can implement logic to detect anomalies or inconsistencies in the received data, triggering alerts or actions as programmed (Figure 5).

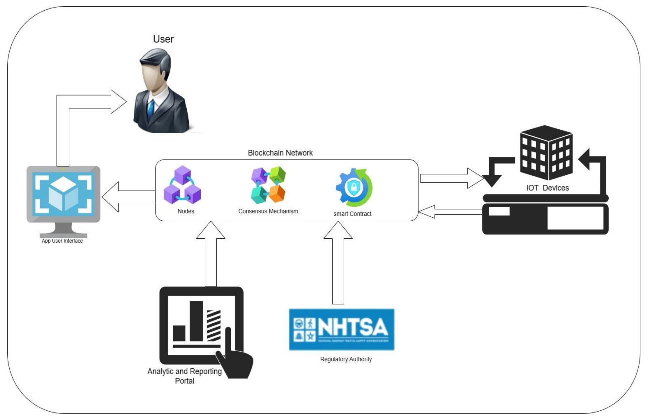


Figure 5: High-level architectural diagram of the proposed solution.

The type of information fed into the system by the IOT device include engine temperature, fuel efficiency and emission level, milage and other information connected to all part of the car. We use three different methods for the data collection which are real-time data streaming, event-driven and periodic data reporting.

All data transmitted from IoT devices is encrypted using robust cryptographic techniques, ensuring data confidentiality during transit. We use a secure communication protocol (like TLS/SSL) to prevent interception and tampering of data in transit. The IoT devices employ strong authentication mechanisms to verify their identity to the block chain network, preventing unauthorized data input.

Key component in the proposed solution

Blockchain network: This is the foundation of the system. It consists of nodes (computers), each nodes indicate the different stakeholders that participate in the block chain network. These nodes maintain a decentralized and secure ledger of vehicle tracking data and also the various stakeholders such as the auto manufactural, car dealers, car owners.

Smart contracts: These are self-executing contracts that govern the rules of the system. The smart contracts can manage data access, validation and reporting.

IoT devices: These devices are installed in vehicles to collect and transmit data to the block chain network. They include GPS, sensors and other relevant components for tracking vehicle-related data.

App user interfaces: User interfaces, which can be web or mobile applications, allow users, administrators and to interact with and access the tracking system. They display real-time data and enable user interactions.

Analytics and reporting portal: These portals enable the generation of reports and dashboards for tracking data analysis. They help in gaining insights into vehicle performance and maintenance needs.

Consensus mechanism: In other to enforce security and trust which is the main focus of this proposal we use the Practical Byzantine Fault Tolerance (PBFT). PBFT mechanisms allow the network to reach consensus even when some nodes fail to respond or respond with incorrect information. BFT enhances the reliability and integrity of the network, making it robust against failure or manipulation by individual nodes. The power consumption of this mechanism is very low which makes it very suitable for this implementation.

Figure 6 below shows the low-level breakdown of the system architecture components and how its integrated with the main vehicle tracking solution.

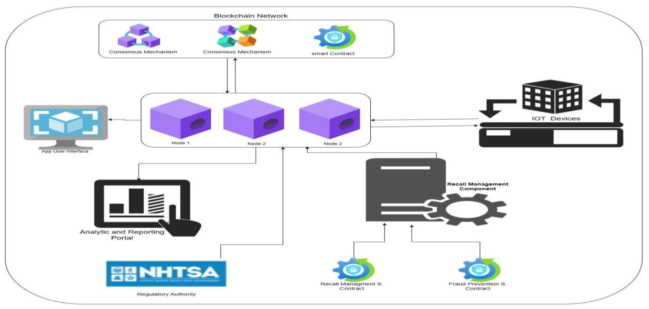


Figure 6: Simplified architectural diagram containing recall component.

The recall management component comprises of.

Recall management smart contracts: This is a smart contract that monitor the block chain ledger for unusual patterns in the input data from the IOT into the block chain. It triggers recall investigation when fault or safety issues are detected.

Fraud prevention smart contracts: These contracts focus on verifying the authenticity of vehicle data, preventing fraudulent ownership transfers and implementing anti-counterfeiting measures.

The recall management and fraud prevention contract interact with the block chain network to enhance vehicle and owner safety, data integrity and prevent fraudulent transaction. This diagram provides a clear high-level view, the implementation will involve more specific details, including workflow processes, regulatory compliance and real-time monitoring which are discussed below [6].

Recall workflow

The workflow process includes (Figure 7):

- Identification of affected vehicle.
- Initiation of recall investigation.
- Generation of recall notice with specific details about the issue.
- Updating of the block chain network, where all the participant in the network get update.
- Updating the block chain with recall status and resolution.

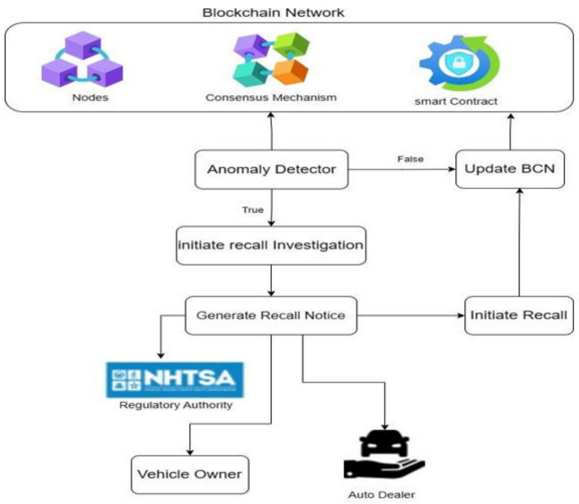


Figure 7: Flow diagram of the recall workflow.

Anomaly detector: The process begins when the system detects anomalies or irregularities in the vehicle tracking data. These anomalies detector is a smart contract that monitors the data from the IOT stored in the Block Chain Network (BCN) to detect potential safety issues with certain vehicles or components.

Initiate recall investigation: If a defect is detected, it automatically prompts the investigation department to carry out investigation. If no defect is detected no action is carried out and it keep monitoring the data from the IOT stored in the Block Chain Network (BCN).

Generate recall notices: The investigation team therefor generate a recall notice to all the stakeholders such vehicle owner, regulatory authority and auto dealers with specific details about the safety issue or defect. These notices may include information on the affected vehicles series, the nature of the problem and recommended actions.

Initiate recall: Affected vehicle owners and dealerships are instructed on how to coordinate repairs or component replacements to resolve the safety issue. The process would be managed efficiently to minimize inconvenience to customers. The block chain ledger is updated with the recall status, indicating which vehicles have undergone repairs or component replacements. This information is stored for transparency and record-keeping.

The block chain network is leveraged to maintain transparency in the entire process. The block chain ledger serves as an immutable record of the manufacturing and ownership history of vehicles and their components, providing a transparent and tamper-proof audit trail. During transfer of ownership the new owner must register using the previous owner wallet address, this is to further enforce security and safety of vehicles.

RESULTS AND DISCUSSION

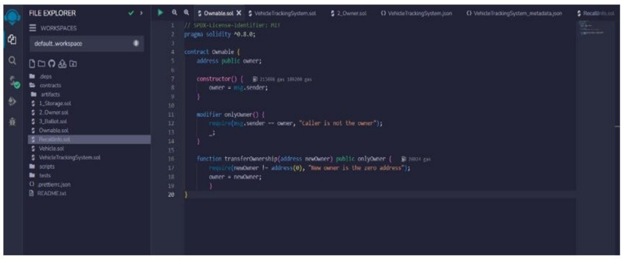
Implementation evaluation

To further illustrate the proposed solution, we did a mock implementation using solidity on remix IDE with Ethereum Virtual Machine (EVM). The screenshot below shows the code and the tested output. The code was written following standard clean architecture with separation of concern approach. Here are the functionalities captured in the smart contract.

- Registering a vehicle and its associated data.
- Updating vehicle data (like location, mileage or maintenance records).
- Handling vehicle ownership transfer.
- Implementing recall functions, allowing manufacturers to issue and manage recalls.
- Enabling access control so that only authorized parties can perform certain actions (like issuing recalls or transferring ownership).

Vehicle owner verification/registration

This module is responsible for the creation of new vehicle owner on the block chain. Before the user is registered the smart contract first do a verification/validation of the user credential (Figure 8).

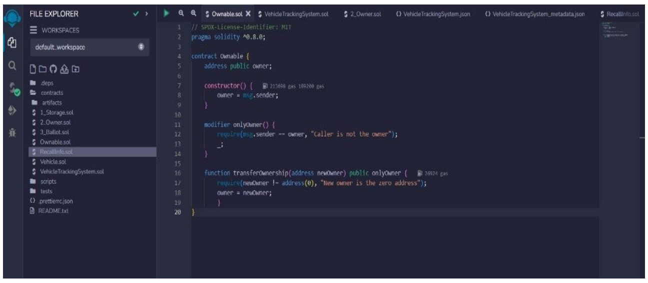


```
// SPDX-License-Identifier: MIT
pragma solidity ^0.8.0;

contract Ownable {
    address public owner;

    constructor() {
        owner = msg.sender;
    }

    modifier onlyOwner() {
        require(msg.sender == owner, "Caller is not the owner");
        _;
    }

    function transferOwnership(address newOwner) public onlyOwner {
        require(newOwner != address(0), "New owner is the zero address");
        owner = newOwner;
        }
}
```

Figure 8: Vehicle owner verification and registration.

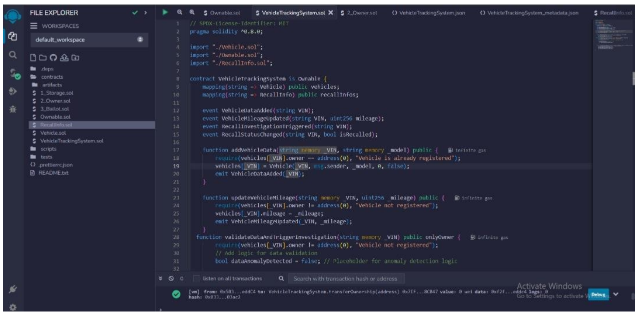
Main solution file

This file contains several functions such as adding vehicle data coming from the IOT device, adding of vehicle milage, data validation for anomalies, resolve recall investigation (Figures 9-15) [7].



```
// SPDX-License-Identifier: MIT
pragma solidity ^0.8.0;

contract Ownable {
    address public owner;

    constructor() {
        owner = msg.sender;
    }

    modifier onlyOwner() {
        require(msg.sender == owner, "Caller is not the owner");
        _;
    }

    function transferOwnership(address newOwner) public onlyOwner {
        require(newOwner != address(0), "New owner is the zero address");
        owner = newOwner;
        }
}
```

Figure 9: Main solution file.

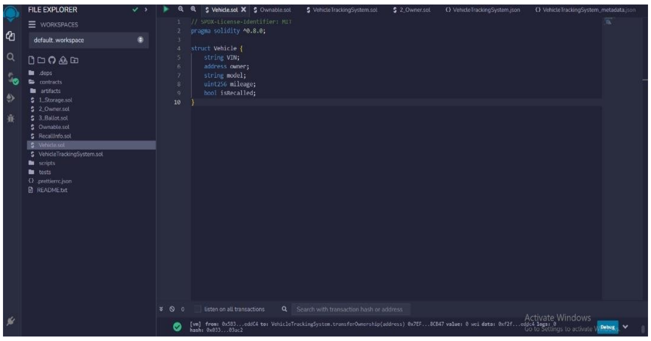


```
// SPDX-License-Identifier: MIT
pragma solidity ^0.8.0;

import "./Vehicle.sol";
import "./Ownable.sol";
import "./RecallInfo.sol";

contract VehicleTrackingSystem is Ownable {
    mapping(string => Vehicle) public vehicles;
    mapping(string => RecallInfo) public recallInfos;

    event VehicleDataAdded(string VIN);
    event VehicleMileageUpdated(string VIN, uint256 mileage);
    event RecallInvestigationTriggered(string VIN);
    event RecallStatusChanged(string VIN, bool isRecalled);

    function addVehicleData(string memory _VIN, string memory _model) public {   infinite gas
        require(vehicles[_VIN].owner == address(0), "Vehicle is already registered");
        vehicles[_VIN] = Vehicle(_VIN, msg.sender, _model, 0, false);
        emit VehicleDataAdded(_VIN);
    }

    function updateVehicleMileage(string memory _VIN, uint256 _mileage) public {   infinite gas
        require(vehicles[_VIN].owner != address(0), "Vehicle not registered");
        vehicles[_VIN].mileage = _mileage;
        emit VehicleMileageUpdated(_VIN, _mileage);
    }
   function validateDataAndTriggerInvestigation(string memory _VIN) public onlyOwner {   infinite gas
        require(vehicles[_VIN].owner != address(0), "Vehicle not registered");
        // Add logic for data validation
        bool dataAnomalyDetected = false; // Placeholder for anomaly detection logic
```

```
[vm] from: 0x5B3...eddC4 to: VehicleTrackingSystem.transferOwnership(address) 0x7EF...8CB47 value: 0 wei data: 0xf2f...eddc4 logs: 0
hash: 0x033...03ac2
```

FILE EXPLORER
WORKSPACES
default_workspace
Ownable.sol
VehicleTrackingSystem.sol
2_Owner.sol
VehicleTrackingSystem.json
VehicleTrackingSystem_metadata.json
RecallInfo.sol
listen on all transactions
Search with transaction hash or address
Debug

Figure 10: Vehicle model.



```
// SPDX-License-Identifier: MIT
pragma solidity ^0.8.0;

struct Vehicle {
    string VIN;
    address owner;
    string model;
    uint256 mileage;
    bool isRecalled;
}
```

```
[vm] from: 0x5B3...eddC4 to: VehicleTrackingSystem.transferOwnership(address) 0x7EF...8CB47 value: 0 wei data: 0xf2f...eddc4 logs: 0
hash: 0x033...03ac2
```

FILE EXPLORER
WORKSPACES
default_workspace
Vehicle.sol
Ownable.sol
VehicleTrackingSystem.sol
2_Owner.sol
VehicleTrackingSystem.json
listen on all transactions
Search with transaction hash or address
Debug

Figure 11: Recall model.

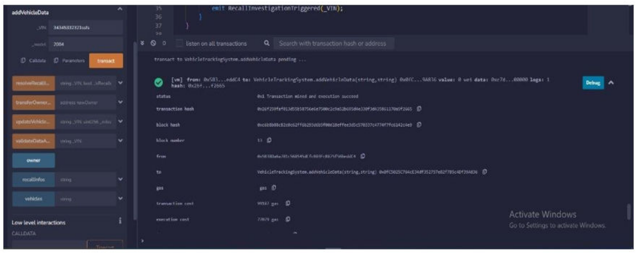
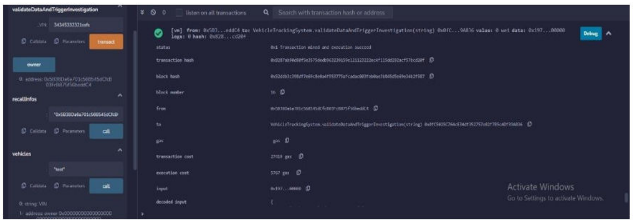


Figure 12: Result of vehicle data creation.



validateDataAndTriggerInvestigation
transact
owner
recallInfos
call
vehicles
listen on all transactions
Search with transaction hash or address
Debug

Figure 13: Result of vehicle data updating.

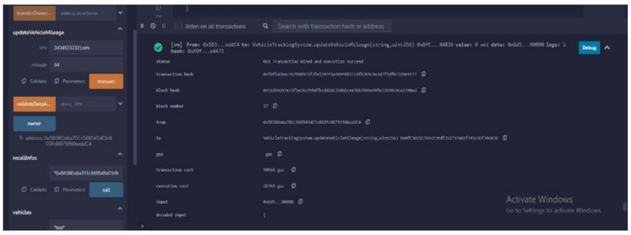


Figure 14: Result of vehicle milage update.

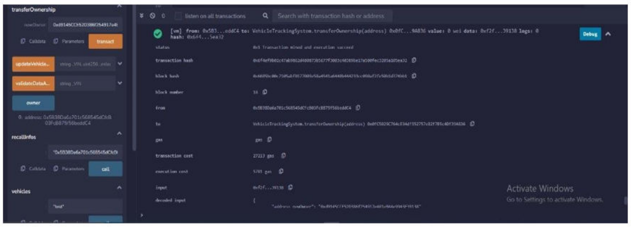


Figure 15: Result of vehicle ownership change.

Here is a link to the written smart contract above.

Model evaluation

We therefore further evaluate the proposed model based on cost implication, security, decentralization, scalability, interoperability compared to existing solution.

Cost implication: The cost implication of this solution varies based on several factors such as development and implementation cost, infrastructure cost, IOT integration, security and privacy measures, scalability and gas fees. The design of the proposed model is simplified to reduce large operations achieving the objective more efficiently which help to reduce operational cost on the user when compared to existing solution.

Security: The proposed model offers a robust security and high-level resilience design. Below are some of the essential security considerations in the proposed models. Data integrity and tamper proof data exploitation is a significant risk to data integrity, which has been mitigated through the use of cryptographic functions in the block chain. The immutability of block chain transactions is achieved through hashing algorithms which ensures that transactions cannot be amended, modified or deleted. This forces stakeholders to digitally sign transactions before they are added to the block chain, further enhancing data integrity.

Availability: The availability of the system to all stakeholders in a secure manner is greatly enhanced by decentralization. Consequently, the likelihood of experiencing Denial of Service (DOS) attacks is highly improbable. Since our system is deployed on the Ethereum machine, stakeholders can always securely access its operations.

Scalability: The system is design using a layered clean code architecture with separation of concern. This separate data processing, storage and interface layers, allowing each layer to scale independently based on demand.

Interoperability: The system is designed to function efficiently while integrating with other systems by distributing the workload across the block chain network consisting of multiple nodes which further enhances scalability [8].

Comparison with other existing block chain-based solution

Researchers have come up with different ideas to solve problems related to recalling products in the automotive industry. However, most of these solutions have not considered important factors like cost and security, except for Fraga-Lamas in his review.

Shafii in their research focuses on the recall of pharmaceutical products, which is different from the recall of automotive products. Another study by looks at the issue of counterfeit automotive parts, which is a major cause of product recalls. However, these studies have not addressed the challenge of single source of operation in the recall process to work together and share information openly in a decentralized block chain [9].

Another study by proposes using block chain technology to track and trace automotive products during a recall. However, this study only involves a limited number of stakeholders, such as the Original Equipment Manufacturer (OEM), supplier and logistics provider and also focuses on vehicle spare parts alone. Our approach, on the other hand, includes other important stakeholders like the customer, dealer and the regulatory authority. This broader approach allows us to manage recalls more effectively [10].

CONCLUSION

The proposed system helps to eliminate fraudulent activities in automobile recall process thereby enhancing the effectiveness of track and trace activities and elements in the automotive recall supply chain. The solution provides efficient tracking of stakeholders and their functions in the automotive recall process, making it applicable to other industries as well.

The issue of security and trust in vehicle recalling automobile industry has been discussed in detail. The introduction, state of the art and related work gave a detail clarification and also provide insight to what other researchers has done previously. We therefore discuss detail solution on how to solve the problem illustrated on the problem statement session. Our solution to the stated problem is discussed in the proposed solution section with a mock implementation to aid technical understanding and implementation of the solution. The security and cost analysis are also provided and further comparison with existing solution was also made to show the novelty in our proposed solution.

RECOMMENDATION

In other to further illustrate the proposed ideal we were able to implement a basic flow of operation. This flow shows the most important functions and models for illustration purpose using remix IDE. In future a detailed implementation of the solution can be done integrating an IOT device installed in a vehicle for real world usage.

Further improvement can also be done in the area of data collection from the IOT device and analysis using Machine Learning (ML) algorithm to improve recall investigation trigger.

REFERENCES

1. Ahsan K, Gunawan I. Analysis of product recalls: Identification of recall initiators and causes of recall. Supply Chain Manag Int J. 2014;7(3):97-106.
2. Ahsan K. Trend analysis of car recalls: Evidence from the US market. Int J Supply Chain Manag. 2013;4(4):1-6.
3. Cardenas-Robledo LA, Hernandez-Uribe O, Reta C, Cantoral-Ceballos JA. Extended reality applications in industry 4.0. A systematic literature review. Telemat Inform. 2022;73:101863.
4. Chi CF, Sigmund D, Astardi MO. Classification scheme for root cause and Failure Modes and Effects Analysis (FMEA) of passenger vehicle recalls. Reliab Eng Syst Saf. 2020;200:106929.
5. Teixeira AA, Moraes TE, Stefanelli NO, de Oliveira JH, Teixeira TB, de Souza Freitas WR. Green supply chain management in Latin America: Systematic literature review and future directions. Environ Qual Manag. 2020;30(2):47-73.
6. Dai B, Nu Y, Xie X, Li J. Interactions of traceability and reliability optimization in a competitive supply chain with product recall. Eur J Oper Res. 2021;290(1):116-131.
7. Ni J, Huang X. Discovery-to-recall in the automotive industry: A problem-solving perspective on investigation of quality failures. J Supply Chain Manag. 2018;54(2):71-95.
8. Sharma PK, Kumar N, Park JH. Block chain-based distributed framework for automotive industry in a smart city. IEEE Trans Ind Inform. 2018;15(7):4197-4205.
9. Wu X, Lin Y. Block chain recall management in pharmaceutical industry. Procedia CIRP. 2019;83:590-595.
10. Yoo SG, Ahn B. A study for efficiency improvement of used car trading based on a public block chain. J Super Comput. 2021;77:10621-10635.