Supply Chain Management on a Block Chain Platform to Improve Quality (Case Study: Saipa Automotive Industries)

Ghazal khodadadi[1], Seyed Zabihullah Hashemi [1*], Sajjad Shokoohyar[2]
1-Department of Information Technology Management Central Tehran Branch, Islamic Azad University, Tehran, Iran
2- School of Management and Accounting, Shahid Beheshti University, Tehran, Iran
* Corresponding author: hashemi_sz@yahoo.com

Abstract

All organizations seek to meet the needs of customers and shareholders; therefore, they need materials, equipment, facilities, and suppliers from other organizations. The performance of an organization is affected by the activities of other organizations forming the supply chain. The efficiency and effectiveness of any organization are the results of the management performance and supply chain structure. In this research, the possibility of using block chain technology in the supply chain process of Saipa Automotive Company has been investigated. This study is descriptive-correlational research and the statistical population of the research is Saipa Automotive Company. The samples were selected by the purposive sampling method. According to the results of the questionnaire distributed in Saipa Company, one of the most important things to examine in the production line of cars based on block chain is the safety of cars, which has been evaluated in the analysis of information. A security mechanism model for the service of connected vehicles using the block chain method is proposed in this study. Data and results analyses using MATLAB software showed that the application of a higher level of supply chain management methods and competitive advantage over improving organizational performance has a significant impact.

Keywords: Supply chain, block chain technology, management, quality

Tob Regul Sci. ™ 2022;8(1): 1385-1400
DOI: doi.org/10.18001/TRS.8.1.108

Introduction

The very survival of today's organizations is dependent upon understanding the needs of customers and responding to these needs quickly. The supply chain includes all activities related to the flow and exchange of goods and services, from the raw material stage to the final product stage which can be consumed by the customer. In addition to material flows, these transfers also include information and financial flows. In a managed supply chain, the manufacturer and its suppliers, buyers, that is, all members of the expanded organization, work together to market a common product or service for which the customer is willing to pay. These partner companies operate as an expanded organization and make optimal use of shared resources to achieve a unique competitive advantage. The result is a high quality product or service (Hosseini et al., 2018).

Decision making is one of the most important stages of supply chain management, which has three main steps. The first step is designing the supply chain strategy, which includes deciding on how to create a coherent structure in accordance with the organization's strategies, as well as identifying the combinations and processes required in each stage (Kumar & Sharma, 2021). The second step is supply chain planning, which involves making decisions and operational policies on how the organizations operate without changing the strategic decisions made in the previous step. The third step is supply chain operations, which involve making decisions and taking steps to better respond to customer-specific orders and needs, which are usually reviewed and decided on a daily or weekly basis (Ellram & Ueltschy Murfield, 2019).

Data authentication, confidentiality, integrity, and privacy are among the key issues related to IoT security. Authentication is required to establish communication between the two devices and to exchange some public and private keys through nodes to prevent data theft.

Block chain technology is essentially a distributed database of documents or the general ledger "of all digital transactions or events", which is run jointly by members. Each transaction is recorded in the general ledger with the consent of the majority of system components (Cagigas et al., 2021). Once entered, the information is never lost, and the block chain records definitive and verifiable information for each unique transaction created. In general, block chain technology consists of a peer-to-peer network combination and the concept of public key and digital signature as well as consensus protocols in which the database automatically monitors and manages information changes. There is no need for an administrator in this network and in fact users perform the management work (Miller, 2018). Block chain has also been described as the most important innovation after the Internet because it can transform the digital world and use the "distributed understanding" feature for any old or current online transaction to execute transactions in such a way that digital assets in the future are also identifiable, and this is done without compromising the privacy and security of digital assets and stakeholders. Data protection and privacy are key challenges for the Internet of Things (Röder & Tibken 2006) Using block chain technology, the problem of identity management in the Internet of Things can be reduced. Trust is an important feature of the Internet of Things, in which blockchain integration can play an important role. Data integration techniques are another option to ensure one-time access to data because they avoid block chain of large amounts of data generated by the Internet of Things.

The automotive sales organization and distribution network have a scattered structure that includes several phases: a central sales department, sales agents in different parts of the world, sales companies in different countries or local regions, and a relatively large number of other retailers. These types of custom cars can only be assembled if ordered. This means that there must be an order by the end customer, retailer, or sales department of the manufacturer that specifies the vehicle options. Current SCM[1] initiatives in the automotive industry seek to increase the share of end customer orders and reduce the share of sales department and retailer orders (Sharma et al., 2018).

[1] Supply chain management

Manufacturers and retailers usually communicate in two rounds. In the first round, a retailer sends medium-term requests to the manufacturer, and they discuss the number of cars the retailer will receive over the next year. Usually this negotiation process is clearly dominated by the manufacturers, in a way that, due to the manufacturer's preferences, the agreed number of cars is less or even more than the original requests. In the second round, about three to five weeks before scheduled production, the retailer must specify options for all of their vehicles that are on time and not assigned to end customer orders. From a retailer's point of view, these cars are based on a kind of predestining process for BTS[1] options. From the manufacturer's point of view, there is an automaker order that justifies the term made to order (Martawati et al., 2020).

The production system in a car assembly plant usually includes four phases: pressing the metal or aluminum sheets; welding the white body of the heated sheets in the body shop; painting it in the paint shop; and final assembly in which the body is painted and engine, transmission, and other equipment are put together or internalized. For the final assembly, one or more production lines are used. As a result, a balanced model composition must be found that uses almost equally different stations on one assembly line (Akafuah et al., 2016).

In addition to the significant intra-organizational information flow between the various automotive self-planning units or departments, there is also the exchange of critical inter-organizational information between the various SC members. Generally, automakers prepare an approximate mid-year supply plan for their suppliers to draw initial attention to potential capacity necks. In short term, daily supply plans are sent to suppliers. These include ordering for the next day as well as very reliable predictions for the following days or weeks and even approximate predictions for the coming months (Schlüter, 2018).

The annual budget plan determines the overall monetary budget of the automotive departments and assembly plants for the following year. To this end, production plans for related factories and sales plans for related sales areas must also be calculated. This step is done once a year. For the next year, it will be implemented on a monthly basis with a decision on the amount of production and sales of the models. It is possible to consider the annual total quantities as next year's volume targets for sales and production. Another result is the annual planning of the budget for the use or reservation of additional capacities until they are affected in the medium term. Due to long lead times, the resources of production resources are usually adapted to customer demand in the long run and are therefore a strategic planning concern. Many other constraints, such as potential suppliers, model combination restrictions, and higher or lower sales bands in certain markets, must be considered. Lower bands, for example, are the result of a strategic guide to presence in important markets. Higher bands may be due to marketing analysis of end costumer demand. The task of planning productive production is similar to planning an annual budget. Again, production and sales plans must be determined and coordinated; however, both require a higher level of detail and are no longer used to derive budget goals (Le Meunier-FitzHugh, 2021). Input data are previously mentioned sales predictions for models and acquisition rate predictions. Due to the high share of end customer orders available for this shorter planning period, these monthly predictions are more reliable than the annual predictions

[1] Base Transceiver Station

used for budget planning. Other input data includes monthly production and sales committees agreed upon in budget planning or related volumes and revenue targets. One goal of productive production planning is to achieve these goals as close as possible in the short term period. The constraints in question are very similar to those related to budget planning. Nevertheless, a higher level of detail is necessary.

The results of productive production planning include updated and more detailed production plans of assembly plants and sales plants. The latter includes values for different sales areas. Due to the above-mentioned constraints, these values may exceed or fall short of the demands of car models originally made by the regions. Perhaps a similar environment of values for sales areas is also part of the annual budget planning. LP[1] and MIP[2] models seem appropriate for productive production planning and budgeting (Fox & Bauldry, 2019). Production plans for automotive models that are the result of annual budgets and productive production planning are the basis for segment demand derivation in the MRP[3] process. Partial demand is transmitted to first tier suppliers as a review of quantities on the verge of delivery in subsequent months. Because car options are only determined for three to five weeks before production, and because the share of final customer orders decreases rapidly for longer driving times. The longer this prediction is expected, the more unreliable it will be. On the other hand, allocation planning should allocate accumulated amounts, which are known as the result of monthly budget planning and consequently weekly productive production planning to the lower levels of the sales system. Depending on the automaker's organizational structure, this planning task may take place at several hierarchical levels, for example, first allocating global quantities to different countries and then allocating these quantities in more detail to the country's retailers and sales subsidizers. After planning the annual budget, the relevant monthly amounts of global areas should be allocated to the countries according to their main requests. If it is not possible to satisfy all the requests, it must be decided who will be satisfied only to some extent. This defect planning follows some predefined rules that, for example, reflect a country's purchasing behavior in the past, or are more or less based on conversations between representatives of global regions and different countries. In addition, the region must balance the deviations of the real demand of the countries from its previous requests between all the different countries assigned to the regions. To this end, the district may also retain a regional group of vehicles not originally requested by any country (Meyr, 2009).

Block chain technology and its impact on infrastructure, supply chains, and business models have exposed the automotive industry to its greatest changes. The influence of new technologies in this industry has facilitated the processes of the automotive industry, accelerated the product life cycle, the dynamics of new business models and increased the diversity of automotive vehicles and services. Has been. At present, main component factories operate in different countries and as a result, supply chain management has been challenged due to the creation of independent systems (Brousmiche et al., 2018). On the other hand, according to

[1] Linear Program

[2] mixed integer programing

[3] Manufacturing resource planning

research conducted in Southeast Asian countries, the level of customer expectations has also increased and car owners are interested in ensuring the quality of production of auto parts, and in the event of any breakdown, the car will be returned immediately. The process of resolving the problems should be visible to them.

At present, some of the largest automotive companies, by understanding the benefits of block chain technology and the power of this technology in facilitating supply chain management, tracking and tracking of parts and products and facilitating the process of applying new standards in automotive industry, seek to apply this technology in complexes. They are themselves. On the other hand, other capabilities of this technology, such as immutability of data and transparency of recorded reports, have accelerated the process of using this technology (Liotine & Ginocchio, 2020).

Using this technology, automakers are able to access all information related to the type and origin of raw materials at different levels of the supply chain, buying and selling raw materials only from the original source. And also have direct control over all interactions and data flows. All of this is achieved through real-time block chain monitoring, smart contracts, and distribution-related features (Liotine & Ginocchio, 2020).

Many major component manufacturers do not have oversight of parts suppliers at the lower levels of their supply chains (level two onwards), and the lack of this oversight extends to raw material supply levels (nth level suppliers). In the absence of the necessary information from the supply chain, such as working capital and levels of financial flows, data analysis is difficult, and this leads to reduced ability of businesses to adapt to change, effective planning and sales of goods and services. By applying block chain-based solutions to supply chain infrastructure, statistical analysis is made more accurate and business relationships become more transparent, which in turn strengthens trust between members and thus facilitates the process of managing supplier relationships.

Wholesale car market, retail and raw material sales can be managed through smart contracts. Intelligent contracts or the same set of autonomous codes can be used in cases such as storing information related to supply and demand (car sales and volume of suppliers' warehouses, sovereignty in the supply of raw materials, equipment, products and services and everything between raw materials Until the end customer is in progress, create and send material purchase requests to be used automatically on sales platforms according to the speed of the production line and the resources available in the warehouses.

In a block chain-based supply chain platform, the following flows are as follows:

- A manufacturer of original parts, to buy raw materials, sends a purchase order with conditions such as favorable price, delivery time, shipping method, place of delivery and other related criteria.
- Suppliers connected to the platform will be notified of the request and they will also announce their terms for delivery of raw materials.
- Finally, the manufacturer of the original parts, either with the help of smart contracts, selects the first offer that is known to be desirable, or manually selects one of the available options.

Research Methodology

Today, many advances have been made in the frontiers of knowledge (Seryasat, O. R., & Haddadnia, J. 2018), (Rahmani-Seryasat, O et all, 2015), (O Rahmani Seryasat, et all, 2016), (Seryasat, O. R., & Haddadnia, J. 2017). Documenting theoretical studies and explaining research hypotheses in two stages to describe the results that follows. The questionnaire was used as a tool to collect data. Data collection was done by distributing a questionnaire directly on the samples and an electronic questionnaire. This questionnaire was divided into two parts, including the factors of acceptance of block chain technology in the process of supply chain of the automotive industry. The questionnaire was measured with a 5-point Likert scale (5 - strongly agree, 1 - strongly disagree). The other part was the respondents' personal information, such as gender, age, and education, type of organization, and position and information technology using behavior among organizations. A questionnaire was used for reliability analysis.

Targeted sampling was used to select and interview the respondents who are in the car supply chain. Examples of managers and staff were first-tier suppliers of auto parts and auto assembly companies. Examples should work in areas that require interaction between organizations and have experience in using information technology between organizations such as sales, purchasing, information technology and engineering. About 385 survey questionnaires were distributed and 261 samples responded to the questionnaire, which shows 79.67%. According to the results of the questionnaire distributed in Saipa Company, one of the most important issues that can be examined in the production line of cars based on block chain was the issue of car safety, which will be evaluated in the analysis of information.

In this research, MATLAB software has been used. MATLAB includes tools that allow programmers to interactively create a graphical user interface. With this feature, the programmer can design complex data analysis programs so that even inexperienced users can easily interact with the program. Under the proposed block chain, each automated vehicle or IoT device is registered on the network before providing or accessing vehicle services. In addition, essential information about vehicles and IoT devices is first entered into a regular database and then stored permanently in a block chain to track the activities of both entities. Figure 1 shows the CAV[1] architecture framework using a block chain technique in which all vehicles are connected to IoT sensors or smart devices to control, monitor and guide drivers on the road. In the proposed framework, the number of vehicles connected to IoT devices or sensors depends on their communication domains and transmissions. Vehicle license plates, rankings given by customers or users with IoT devices are stored in regular tables as well as in the block chain network to track and record any legal or illegal activity of the vehicle or IoT devices. In the case of any device compromised by intruders, the relevant authorities who are part of the block chain are able to identify and take immediate action against the IoT device. Instead of registering IoT devices, it is possible to track, analyze and register any vehicle in the block chain. However, keeping records of this massive vehicle data during their mobility in real-time scenarios increases the likelihood of power and computational time. As a result, to limit computing power and storage, recording, analyzing, and storing only the activities of IoT devices in the block chain can be easy. Devices

[1] Connected and Autonomous Vehicles

that track a certain number of vehicles and provide services at the user's request can be easily tracked and registered in the block chain. It is possible to use any IoT device containing vehicle records and provide services to different vehicles in the form of search information for storage in the block. Any change in the transfer of information on vehicles or devices by intruders is able to change the history or transactions that further penalize the devices or vehicles by blocking or reducing vehicle ratings.

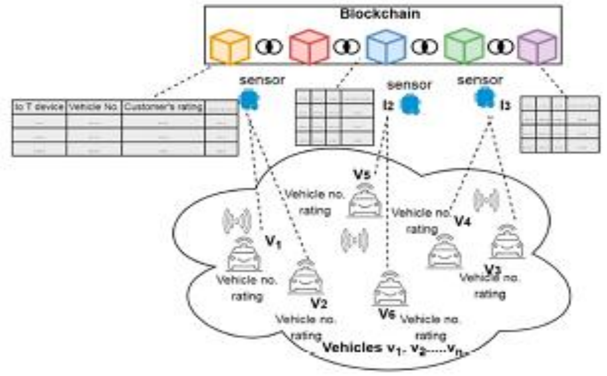

Figure 1. Connected vehicle block chain architecture framework

To ensure safety and transparency during driving, any IoT device that provides vehicle information registers with the block chain network before providing services to vehicles. In addition, any license plates or vehicle ratings given by customers are stored in the block chain network. In CAV, smart objects continuously monitor and control taxi services, and each IoT device is authenticated with a counterpart in the block chain network, as shown in Figure 2.

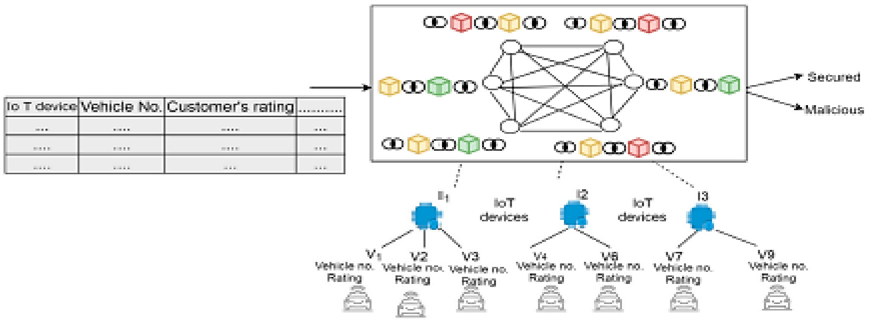

Figure 2. Block chain network

A block chain network is a combination of peer-to-peer and probe nodes that are responsible for generating cryptographic keys and authenticating the vehicle or new IoT device connected to the network to avoid network failures. More than one administrator is selected to ensure network security for a specific period of time. When the manager is selected, the secondary block chain manager is selected to recover from the failure of the primary manager. All IoT devices or vehicles are registered in the block chain network by submitting a subscription request to the peer manager.

Each vehicle acts as a node connected to its common or close counterpart nodes. The proposed flowchart framework is shown in Figure 3. As shown in Figure 3, whenever user X needs to reserve a navigation, he requests navigation by sharing time, pickup and drop-off points. In this study, users or customers are considered legitimate and do not need to express their identity in the block chain network. This driving request is visible to all registered providers on the network who are part of the block chain. A driver gets positive or negative reviews from other users based on their behavior. Various parameters are used to calculate provider ratings, including the trust or rating factor. A provider with a high trust or rating factor is considered to have the highest degree of trust. The user chooses their provider depending on the rating or trust factor. In taxi forwarding services, various communications take place between the service provider and the requester. If provider Y wishes to respond to this request, it will be able to share its intention with X.

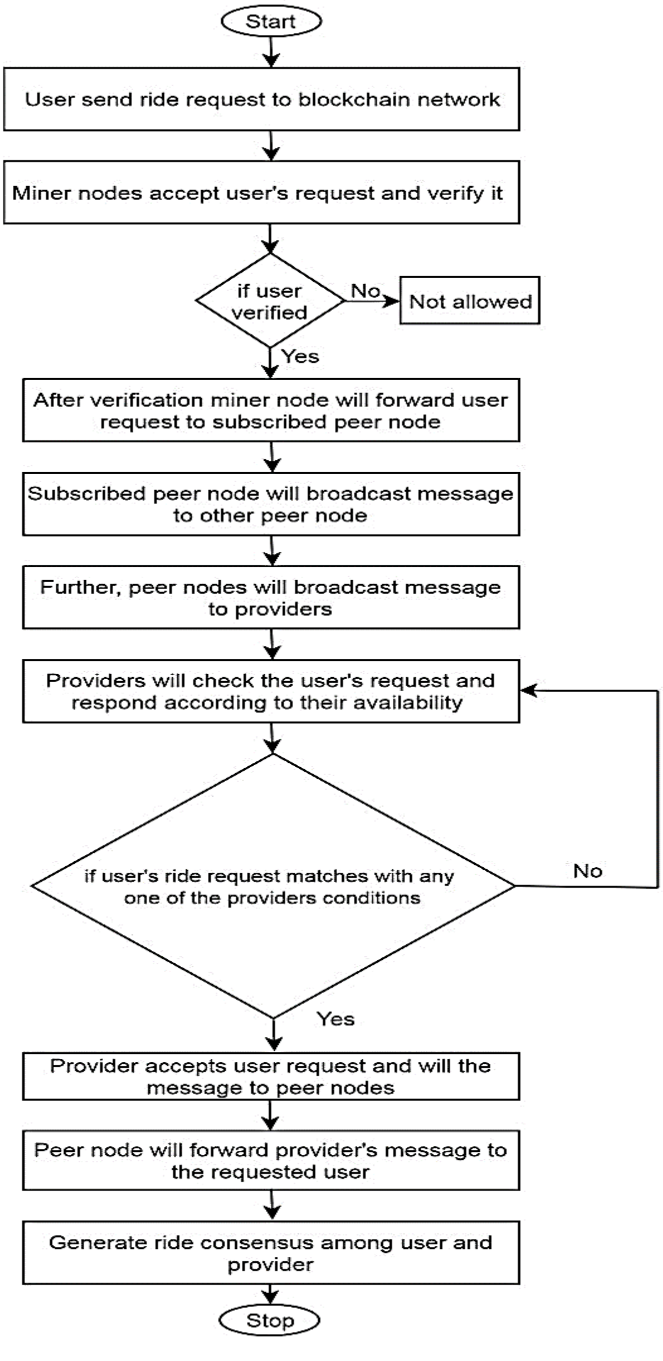
Start
User send ride request to blockchain network
Miner nodes accept user's request and verify it
if user verified
No
Not allowed
Yes
After verification miner node will forward user request to subscribed peer node
Subscribed peer node will broadcast message to other peer node
Further, peer nodes will broadcast message to providers
Providers will check the user's request and respond according to their availability
if user's ride request matches with any one of the providers conditions
No
Yes
Provider accepts user request and will the message to peer nodes
Peer node will forward provider's message to the requested user
Generate ride consensus among user and provider
Stop

Figure 3. Workflow of the proposed framework

Provider Y selects the response to the navigation request based on certain criteria, such as the user path, in which if the travel path Y matches the X path, then Y accesses the navigation request. Whenever user X or provider Y agrees to the redirect request, it is possible to maintain a block chain with a hash so that it is possible to detect any misbehavior or change in peak position or drop point on the network. Figure 4 is drawn. Each block consists of information about IoT devices attached to the previous block through a hash, which is shown in Figure 5 so that any changes or deletions of any intrusive information can be detected by other devices.

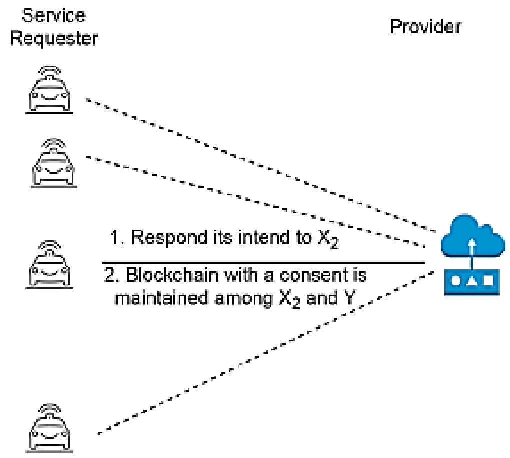
Service Requester
Provider
1. Respond its intend to X_2
2. Blockchain with a consent is maintained among X_2 and Y

Figure 4. Satisfaction through the block chain between the provider and the requesting guide

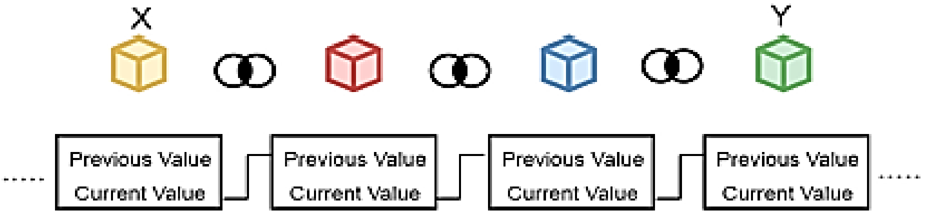

Figure 5. Block chain between transmitter and receiver

Attack scenarios

Whenever an attacker wants to carry out malicious activity on the network, he implements a number of attack strategies. Endangering IoT devices or sensors, changing rankings given by drivers, denying data, and traffic volume are some of the things that can be easily generated by an intruder for personal gain. The attack scenarios that are possible during the driving service between the user and the vehicle are described in detail below. Adding an IoT compromised by an intruder: When an IoT intruder registers itself at risk for active or passive attacks, block chain counter-nodes immediately investigate illegal actions such as theft or compromise. Legitimate IoT devices identify them.

User misconduct: For example, a user named Alice requests a ride and a taxi driver agrees to drive. However, while driving, the provider starts abusing the user by changing the user's preferred route, Alice, or by making unnecessary stops. IoT sensors, which continuously monitor or track the location of the taxi, take steps to prevent malfunctions for the user. At the same time, the taxi driver must be at the end of the sentence with a demotion or other necessary action.

Change of ratings: Once the ratings have been stated corresponding to each taxi driver, it is not possible to change it even after the IoT devices have been successfully compromised.

Data Denial Attack: This is one of the main security issues in CAV in which vehicles depend on information received from vehicles or other counterparts.

Traffic volume: In this case, intruders try to divert route offers on the roads for their own benefit. However, to prevent these attack strategies, this study proposed a mechanism for the safe sharing and routing of taxis through the block chain. In addition, to validate the proposed mechanism, numerical simulations are performed on various parameters that show the improvement of the proposed framework.

Performance analysis

To validate the proposed framework, CAV block chain framework simulation using block chain technique through NS2[1] simulator has been ensured. In this study, the probability of impending attacks on IoT devices or vehicles of the proposed framework is analyzed. First, a network area of 700 by 700 meters with a network size of 50 nodes was created, in which vehicles have a dynamic nature and are able to join any range of other devices, which is presented in Table 1. To establish the network facilities, the initial random rating or TF[2] was assigned to each device or vehicle on the network and five nodes were created that act as block chain nodes. To measure the validity of the proposed phenomenon, performance against several security metrics was measured, including changing the user's false message, the likelihood of an attack on IoT devices, and changing user history information such as rankings. To measure the validity or validation of the proposed CAV block chain framework, the NS2 simulator was used, in which the number of attack scenarios on IoT devices was considered. The attack scenario or conflict model of the proposed framework is illustrated in Figure 6, in which hackers compromise IoT devices by impersonating legitimate devices or hacking legitimate IoT sensors on the network. To validate or measure the eligibility of the proposed phenomenon, attack nodes were added at a rate of 10% for legitimate nodes in the network.

Table 1. Parameters

Number of Nodes in a CRN	25, 500
Grid facet	700 × 700 m
Transmission Range	140 m (approx.)
Data Size or users request	256 Bytes
Simulation time	80 s
Physical Layer	PHY 802.11

[1] Network Simulator

[2] Term Frequency

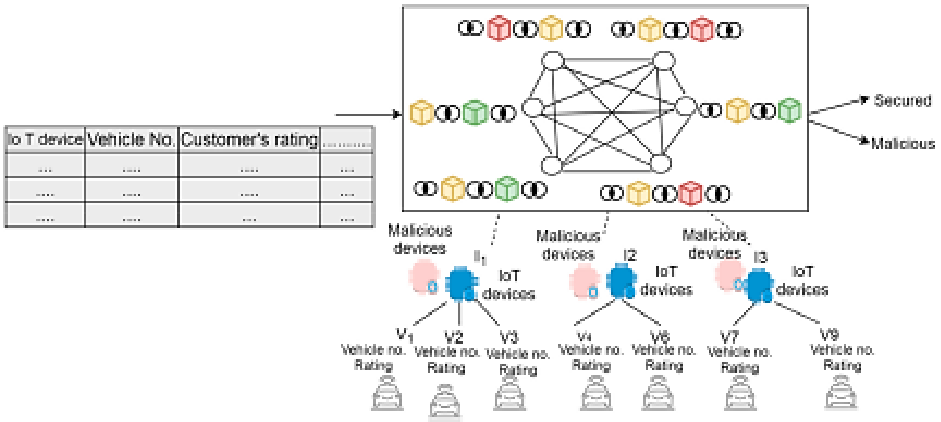

Figure 6. Conflicting network model of the proposed phenomenon

Hackers who try to compromise IoT devices by hacking the identities of legitimate devices to carry out human attacks or behave like legitimate devices are considered to be the proposed framework for analysis. In addition, the proposed phenomenon of network congestion and the ability to compromise has been confirmed in which intruders consume network resources by issuing false requests. In addition, the proposed framework was measured against possible authentication scenarios in which attackers attempted to compromise IoT devices and demonstrated how to analyze and measure the possibility of attacks in which IoT intruders Endanger. Proposed phenomenon the values of the false, extinct, and correct authentication scenarios showed how the proposed phenomenon effectively measured attacks in which intruders compromised devices. In addition, malicious devices or nodes in the network based on the normal distribution during the communication process were added to validate the framework against threats. In addition, the proposed block chain environment is a combination of probes and peer nodes to validate and add new nodes (devices) to the network. Among them, some probe nodes also became malicious nodes to observe the security recovery process. In addition, IoT devices were considered a threat to intruders. The IoT invasion showed that in the individual time unit, 2 out of 5, 10 out of 20 and 20 out of 50 devices were compromised, as shown in Table 2. In addition, the user's false request was considered another threat in which the addition of a false request by hackers caused congestion in the network. Considering all these hypotheses, the performance analysis was performed for 60 seconds. The proposed framework was validated and compared against the conventional approach, which is discussed below.

Table 2. NS2 configuration for different network environments

S. No.	Transmitting Nodes	IoT Nodes	Compromised Miners	Attack Probability
1	25	5, 10, 20	2, 10, 20	5%
2	100	25, 50, 75	15, 25, 50	25%

Available method

(Rawat et al., 2017) demonstrated the threat of data denial by using hashes to enhance network performance and security by adapting the conflict window size to disseminate accurate information to neighboring vehicles. In addition, the authors proposed a clustering scheme to overcome travel time during traffic congestion. The existing mechanism was validated through numerical results obtained from virtual simulation. The proposed paper analyzes the IoT block chain mechanism for CAVs on various networking parameters including false user requests, compromising IoT devices, and changes in user stored rankings. The proposed framework was measured in front of (Rawat et al., 2017) in which the authors ensured security by generating hashes of information transmitted between institutions. However, it is possible to hack and easily change encrypted messages by hackers. In addition, individual change or compromise of IoT devices in the CAV network may be unaware of the entire network. However, in the mechanism proposed in this study, the individual change in each device or information immediately changes the remaining networks.

The results of the proposed phenomenon were measured against two attack scenarios, namely network congestion and the ability to compromise, which were further compared to the existing approaches described in Section a of Section 4. The proposed method seeks to enhance vehicle security through block chain, in which each IoT device is recorded and analyzed to detect the potential threat. On the other hand, (Rawat et al., 2017) proposed a phenomenon in which the hash chains of each vehicle are recorded in the network, which may increase the likelihood of attack due to network congestion and lower computing power of the vehicles. Experimental evaluation of conventional and proposed approaches has been successfully achieved and multiple results have been recorded according to different parameters. The results of system mode and performance parameters are presented in the previous sections of Performance Analysis. The system behaved as expected and all performance parameters for each CAV data were positive for the proposed framework. Mobility and activity recording are performed by IoT devices that are static and capable of effective analysis and detection. The movement of vehicles allows for a new connection to the IoT device of their suffering, in which the devices work together to further analyze their interactions.

In addition, the accuracy of the proposed approach was close to 86%, which improved over time due to the removal of detected malicious nodes from the system. Detection of malicious nodes is based on trust, in which the removal of detected malicious nodes does not prevent the operation of other nodes. The proposed mechanism calculates the trust of other nodes after each specific time period in which the nodes are endangered and have lower destructive behavior and trust due to high production drop rates, black holes and false attacks. They will never be considered in the future. The results showed the improvement of the proposed mechanism against the existing approaches with a success rate of 86%. If the experimental test lasts longer, it can be further developed. The measurement parameters performed better in the proposed framework compared to the existing systems. In addition, it is possible to further improve the accuracy of the resulting framework over time by removing the detected malicious nodes from the network. Detecting malicious nodes following their removal does not alter trust or prevent other nodes from functioning. The proposed mechanism calculates the trust factor of its nodes after a certain period of time. Endangered and malicious nodes have lower ratings and trust and are never considered to form a path. In all graphs drawn from Figures 8 to 10, the proposed security framework promotes better results than existing mechanisms. In the case of the user false request graph shown in Figure 7, corresponding to the network congestion, the existing scheme works less efficiently as the number of false requests increases with the network size. The congestion of false requests increases the network overhead and the communication between sender and receiver and makes it difficult to maintain. In addition, increasing network congestion consumes essential resources, which further leads to a significant reduction in network performance. In addition, corresponding to endangered devices, the control and monitoring mechanism of the data was greatly affected, as shown in Figure 8. In the case of compromised IoT devices, hackers not only affect network performance, but also gain access to restricted areas or steal confidential information for their own benefit. However, in the case of Figure 9, hackers change users' stored rankings and continue to abuse their customers.

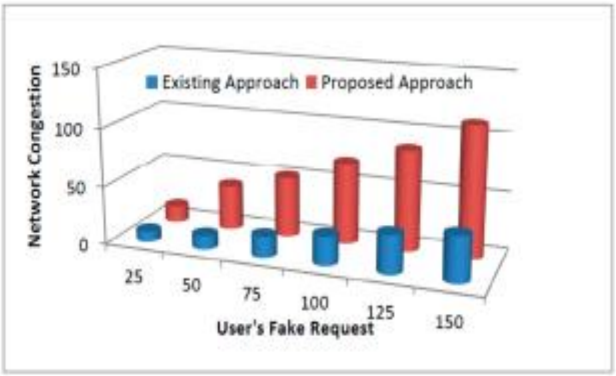

Figure 7. False requests of users corresponding to network congestion

With block chain technology, all the necessary records of documentation or monitoring or control are stored in the block chain so that the change, deletion, modification or compromise of any IoT device is quickly monitored and for other devices to provide or prevent Identify possible future injuries. In the proposed phenomenon, the vehicle security framework was delineated with the block chain technique, which improved network performance and secured online taxi services. The performance analysis of the proposed framework was described in more detail along with the approval times depending on the different possible attack strategies. Figure 10 outlines possible strategies for false, extinct, and correct authentication, and shows the validation of the proposed phenomenon with false requests and the ability to take risks. It is possible to apply this approach effectively in real-time scenarios by measuring the likelihood of an attack.

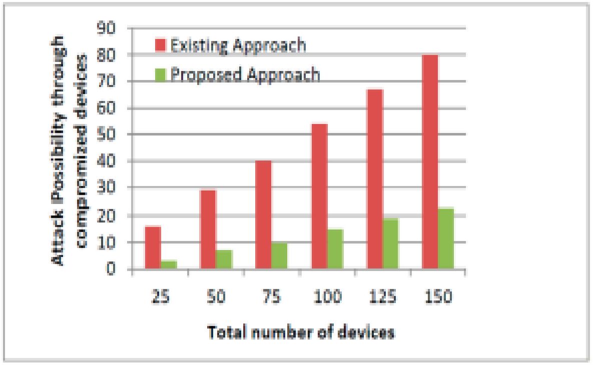

Figure 8. Possibility of attack on compromised devices

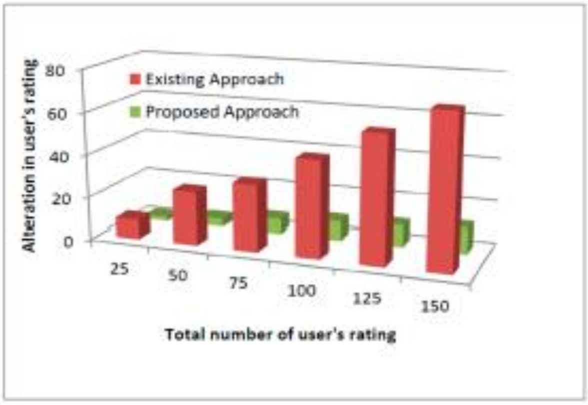

Figure 9. Rankings stored within the user by intruders

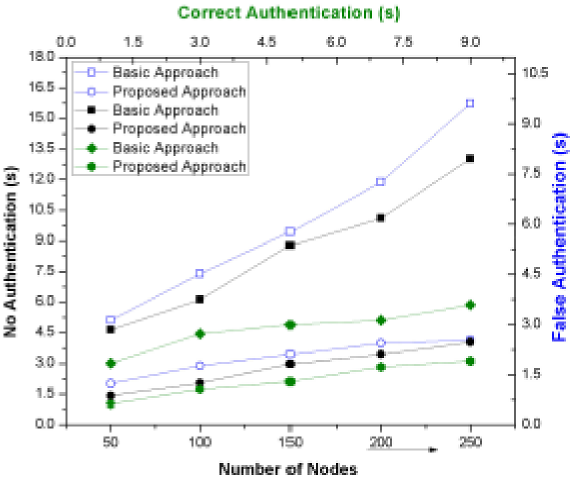

Figure 10. Probable attack scenarios

Conclusion

In this research, IoV[1] program is considered and a security mechanism is proposed for the service framework of connected autonomous vehicles using blockchain method. In order to ensure confidentiality and transparency among customers and cabin drivers, any activities related to vehicles or IoT devices are tracked and recorded within the blockchain. The blockchain mechanism is used to extract information from IoT devices and store the extracted records to ensure customer safety and device security by creating transparency between different authorities. The proposed framework significantly reduced users' fake requests, compromises on IoT devices, and changes in stored user ratings. The simulated results against different parameters show 79% success in the proposed framework compared to the existing approach against the mentioned parameters. The proposed phenomenon against more nodes and transaction change already stored in the blockchain network will be reported in future communications. In addition, technology including deep and enhanced learning will be adapted to increase system intelligence. In future research, other existing issues such as automatic connection and automatic car charging can be followed in case studies of electric hybrid vehicles. Also, the results and methods proposed in this research can be used in the production line and car repairs based on what is affected in the

[1] *iov*-blockchain

questionnaire as the most important factor in car production. In future research, methods based on optimization algorithms and fuzzy neural networks can be used to improve the results.

Declarations

Funding (Not applicable)

Conflicts of interest/Competing interests (The authors declare that they have no conflict of interest)

Availability of data and material (Not applicable)

Code availability (Not applicable)

Authors' contributions (All authors contributed to the study conception and design. Material preparation, data collection and analysis were performed by [Authors 1], and [Author 2]. The first draft of the manuscript was written by [Authors 1] and all authors commented on previous versions of the manuscript. All authors read and approved the final manuscript.)

References

1. Akafuah, N., Poozesh, S., Salaimeh, A., Patrick, G., Lawler, K., & Saito, K. (2016). Evolution of the Automotive Body Coating Process—A Review. Coatings, 6(2), 24.
2. Brousmiche, K. L., Heno, T., Poulain, C., Dalmieres, A., & Hamida, E. B. (2018, February). Digitizing, securing and sharing vehicles life-cycle over a consortium blockchain: Lessons learned. In 2018 9th IFIP international conference on new technologies, mobility and security (NTMS) (pp. 1-5). IEEE.
3. Cagigas, D., Clifton, J., Diaz-Fuentes, D., & Fernandez-Gutierrez, M. (2021). Blockchain for Public Services: A Systematic Literature Review. IEEE Access, 9, 13904–13921.
4. Ellram, L. M., & Ueltschy Murfield, M. L. (2019). Supply chain management in industrial marketing–Relationships matter. Industrial Marketing Management, 79, 36–45.
5. Fox, W. P., & Bauldry, W. C. (2019). Problem Solving with Linear, Integer, and Mixed Integer Programming. Advanced Problem Solving with Maple™, 139–206.
6. Hosseini, A., Soltani, S., & Mehdizadeh, M. (2018). Competitive Advantage and Its Impact on New Product Development Strategy (Case Study: Toos Nirro Technical Firm). Journal of Open Innovation: Technology, Market, and Complexity, 4(2), 3.
7. Kumar, B., & Sharma, A. (2021). Managing the supply chain during disruptions: Developing a framework for decision-making. Industrial Marketing Management, 97, 159–172.
8. Le Meunier-FitzHugh, K. (2021). 7. Product, new product development, and service marketing. Marketing: A Very Short Introduction, 97–113.
9. Liotine, M., & Ginocchio, D. (2020). The supply blockchain: integrating blockchain technology within supply chain operations. Technology in Supply Chain Management and Logistics, 57–89.
10. Martawati, M. E., Rohman, F., Kurniawan, H. F. D., & Abidin, I. N. (2020). The effect of distance Base Transceiver Station (BTS) on speed of vehicle safety response based on internet of things. IOP Conference Series: Materials Science and Engineering, 732, 012083.
11. Meyr, H. (2009). Supply chain planning in the German automotive industry. In Supply Chain Planning (pp. 1-23). Springer, Berlin, Heidelberg.

12. Miller, D. (2018). Blockchain and the internet of things in the industrial sector. IT professional, 20(3), 15-18.
13. O Rahmani Seryasat, J Haddadnia, H Ghayoumi Zadeh, Assessment of a Novel Computer Aided Mass Diagnosis System in Mammograms, Iranian Journal of Breast Disease 9 (3), 31-41, 2016
14. Rawat, D.B.; Garuba, M.; Chen, L.; Yang, Q. On the security of information dissemination in the Internet-of-Vehicles. Tsinghua Sci. Technol. 2017, 22, 437–445. [Google Scholar] [CrossRef]
15. Rahmani-Seryasat, O., Haddadnia, J., & Ghayoumi-Zadeh, H. (2015). A new method to classify breast cancer tumors and their fractionation. Ciência e Natura, 37(4), 51-57.
16. Röder, A., & Tibken, B. (2006). A methodology for modeling inter-company supply chains and for evaluating a method of integrated product and process documentation. European Journal of Operational Research, 169(3), 1010-1029.
17. Schlüter, F. (2018). Procedure Model for Supply Chain Digitalization Scenarios for a Data-Driven Supply Chain Risk Management. Revisiting Supply Chain Risk, 137–154.
18. Sharma, P. K., Kumar, N., & Park, J. H. (2018). Blockchain-based distributed framework for automotive industry in a smart city. IEEE Transactions on Industrial Informatics, 15(7), 4197-4205.
19. Seryasat, O. R., & Haddadnia, J. (2018). Evaluation of a new ensemble learning framework for mass classification in mammograms. Clinical breast cancer, 18(3), e407-e420.
20. Seryasat, O. R., & Haddadnia, J. (2017). Assessment of a novel computer aided mass diagnosis system in mammograms. Biomedical Research (0970-938X), 28(7).