Research Article

An Internet of Things (IoT) Based Block Chain Technology to Enhance the Quality of Supply Chain Management (SCM)

Ali Rizwan [ID],[1] Dimitrios A. Karras,[2] Jitendra Kumar,[3] Manuel Sánchez-Chero [ID],[4] Marlon Martín Mogollón Taboada,[5] and Gilder Cieza Altamirano [ID][6]

[1]*Department of Industrial Engineering, Faculty of Engineering, King Abdulaziz University, Jeddah 21589, Saudi Arabia*
[2]*School of Science, National and Kapodistrian, University of Athens (NKUA), Athens 34400, Greece*
[3]*Department of Electronics and Communication Engineering, GLA University, Mathura, Utter Pradesh, India*
[4]*Facultad de Ingeniería de Industrias Alimentarias y Biotecnología, Universidad Nacional de Frontera, Sullana, Peru*
[5]*Facultad de Ciencias Empresariales y Ambientales, Universidad Nacional de Frontera, Sullana, Peru*
[6]*Universidad Nacional Autónoma de Chota, Cajamarca, Peru*

Correspondence should be addressed to Ali Rizwan; arkhan71@kau.edu.sa

Recent technological developments indicate possible advancements in supply chain management (SCM). These innovations have attracted a lot of interest from industries including logistics, manufacturing, packaging, and transportation. The conventional systems, however, use centralised servers to control all operations, including the exchange of raw materials, making orders, dealing with buyers and sellers, and updating orders. The network's supply chain may thus be insecure as a result of every activity being routed via centralised servers. The danger is additionally increased by a number of difficulties, including scalability, data integrity, security, and availability. Block chain technology may be used in these circumstances to decentralise transaction processing and eliminate the need for a centralised controller. In this approach, the performance of the resource-constrained supply chain network is improved by the effective use of edge computing and priority data access. The Intelligent *K*-Means (IKM) clustering algorithm is suggested across the edge nodes in the current research to categorise the priority level of each piece of data. This classifier determines if the edge node has received data that is high priority or low priority. Low priority data is recorded in the log files for future data analysis. Then, to allow safe data flow in the open block chain while excluding outside parties, the High Priority Access based Smart Contract (HPASC) technique is deployed. The whole experiment was conducted in a Python environment, and variables including scalability, reaction time, throughput, and accuracy were studied. Current systems' constrained block sizes and fork creation lengthen the time transactions must wait before being processed. The suggested methodology is quicker and uses less storage space than current block chain systems. The results show that the suggested approach works better than current blockchain technology to raise the standard of supply chain management.

1. Introduction

Due to technology improvements over the previous several decades, outdated systems were replaced by smart devices. Similar to this, automated systems for monitoring, uploading food stockpiles, making orders, and handling financial transactions have replaced the conventional Excel systems used in supply chain operations. In a small-scale company, managing the supply chain process is considerably more difficult since it requires complete web access to the core component. SCM becomes more active in optimising customer value and dependability as a result of the development of smart solutions like enterprise resource planning, smart logistics, and online tracking. SCM reveals informational and physical fluxes. While the latter performs buyer-seller contact and live-stock monitoring from production to consumer, the former deals with vehicle mobility and storage management. The modern supply chain systems

have to deal with a number of difficulties, including asset tracking, scalability, resource constraints, and information hacking. To address these issues, a number of researchers have put forward several methods [1]. But there is still a problem with finding the best option for an effective SCM. One of the technologies used in conjunction with business logic to carry out smart contracts that deal with product licencing improved asset monitoring, and security transparency is blockchain. By using a public ledger system to continuously record shipping containers, monitor inventory, and manage tax bills and payments, block chain technology may also be used to logistics.

It also lays the way for a genuine, scalable solution for SCM procedures. According to a 2019 assessment, Zeto, Modum, Waltonchain, Ambrosus, and Devery are a few examples of blockchain SCM initiatives that have found success. Generally speaking, SCMs often rely on centralised servers for processing, which lower network throughput and processing power. As a result, depending only on cloud computing is not an ideal option. A developing technology called edge computing makes it possible for edge nodes to carry out computation. The main goal of edge computing is to distribute certain jobs from cloud servers to the participating edge nodes in order to lessen the strain on the central point. Block chain can provide secure and dependable SCMs because of its distributed environment. Although the edge-block chain has several benefits over current SCMs, there is still need for development in areas like scalability, privacy, energy use, and security. There have been several scalability measures implemented, and some of the shortcomings of such studies are given here.

(i) The large data processing in a resource-constrained setting is not addressed by the current scalable blockchain approaches.

(ii) Uploading a lot of data to the cloud servers could cause congestion and use up additional bandwidth.

(iii) Using greater processing resources to handle all types of data sent over the SCM network.

Furthermore, there is no precise answer that more closely meets the requirements of contemporary SCMs. In order to address these issues, this study proposes an intelligent automated method for scalable food traceability. Due to its effective work automation, machine learning (ML) technologies have made great strides in recent years, drawing interest from a variety of groups [2, 3]. In order to shorten the computation time across the edges, the present study divides the data into two groups, "prioritised" and "low-prioritized," using an intelligent clustering approach.

1.1. Contribution of the Study

(i) Edge nodes are presented to categorise the priority level of each data using the Intelligent K-Means (IKM) clustering approach.

(ii) Data transfer on the public blockchain is safeguarded via the High Priority Access Smart Contract (HPASC) approach.

(iii) Scalability, reaction time, throughput, and accuracy were all measured in this study, which was carried out entirely in a Python environment.

(iv) Compared to current block chain systems, the suggested approach is quicker and uses less storage space.

1.2. Motivation of the Study.
Lack of technical know-how and understanding of blockchain technology's applications serve as a barrier to the supply chain's adoption of this new technology. Blockchain is gaining popularity in the technical community; however, there are not many applications or technical developers yet, which is a problem. Information technologies such as blockchain may be disruptive and call for the replacement or alteration of existing legacy systems.

Additionally, each edge stores the low priority data in log files for later analysis. Because the blocks only contain the priority data, the suggested system has great scalability. Additionally, by processing the data according to its priority, it works better in a setting with limited resources. The ML-based priority classification gives increased scalability and availability measures since it defines the classes of the training data among the edge nodes.

2. State-of-the-Art Analysis

The following explores the existing studies that prevailed in supply chain management using blockchain. Also, it presents recent state-of-art methodologies to overcome scalability issues in blockchain networks. Alzahrani and Bulusu [4] propose a technique to employ NFC tags to track and trace the products over the supply chain networks [4]. They highlight some of the key features such as security, storage efficiency, and location tracking using Unique ID (UID). Later, Kefalakis et al. [5] develop an object tracking using NFC tags comprising a list of tagged objects [5]. They develop a handheld device to pick up the list of intended objects in the goods. Furthermore, the research enforces blockchain to promote secure data transfer over the network. As advancement over the UID-based supply chain, the authors have developed an RFID-based strategy for monitoring transportation in the entire SCM network [6, 7]. Also, the article [8] ascertains for detecting the counterfeit product in the SCM process using RFID tags. Recent researchers suggested implementing blockchain functionalities in the SCM processes. In this context, an Agri-based traceability system proposed by authors highlights the importance of blockchain when combined with the RFID tags [9]. This study encapsulates food safety and traceability in food supply chain networks. Later, the authors propose a mechanism to achieve transparency throughout the SCM network. They adopt EPC global network for the effective use of RFID in the garment supply chain [10]. As an enhancement, Zhao et al. suggest an SCM using blockchain and distributed ledger for a globally connected supply chain framework [11]. Followed by Zhao et al. [11], researchers present a novel "Blockchain-as-a-Service" to provide insights for deploying blockchain in IoT networks [12, 13].

Also, blockchain in intelligent transportation systems has made remarkable achievements [14, 15]. In recent decades, blockchain increasingly combined with edge computing to overcome the problems such as response time, network pressure, and security. The security in edge computing is increasingly exposed due to data tampering, data destruction, and data leakage [16, 17]. As an innovation, blockchain stores the information and transactions over the peer-to-peer networks [18]. In some applications, machine learning algorithms are applied effectively to classify special device information to achieve scalability and security [19]. Many researchers have proposed many solutions for scalability enhancement in the blockchain. For instance, a chain-partitioned scalability mechanism is put forth in literature [20]. In this study, on-chain, off-chain, and side-chain structures are established to increase the throughput and transmission rate during reduced block size. Additionally, in DAG-based scalability, the authors design a graph-based blockchain where the vertices represent the contracts and edges represent the interactions [21]. Here, partitioning is performed where the partition is balanced by minimizing the edges in the blockchain network to achieve scalability. Furthermore, the sharing mechanism is practiced in many blockchain networks where the database splits horizontally to spread the nodes.

3. Theoretical Framework

In this section, we consider sea food supply chain management in which edge-based block chain scheme encompassing priority-based access scheme to achieve scalability. Figure 1 depicts the sea food supply chain management. Consider a supply chain environment comprising of following activities: (i) Raw material supply, (ii) Production encompassing accurate planning and inventory management, (iii) processing the sea food followed by packaging, (iv) Efficient storage, and (v) Distributing the sea foods to the end users (wholesale/retail).

If the aforementioned activities are not handled properly, the entire SCM will fail which in turn leads to the loss of faith on company and food quality. Meanwhile, the deployed IoT sensors collect operational data from each division and transfer the data over the network to perform real-time monitoring of sea foods. It often requires RFID to check whether the sea food products are counterfeit or not [22, 23]. The edge nodes collect and analyze the data received from diverse ends of the supply chain management.

Figure 2 depicts the system flow of the proposed SCM processes. While edge computing exclusively refers to compute at the ingress of the network, fog computing is inclusive of computing anywhere along the continuum, from cloud to the edge. Block chain coupled with edge computing can provide fairness in end-user experience and scalable infrastructure. The underlying decentralized and distributed edge platform perform simulation of block chain. Each edge node effectively does the storage and information exchange for reducing the burden of computing load and memory consumption while handling superfluous information. The primary objective of the proposed SCM is
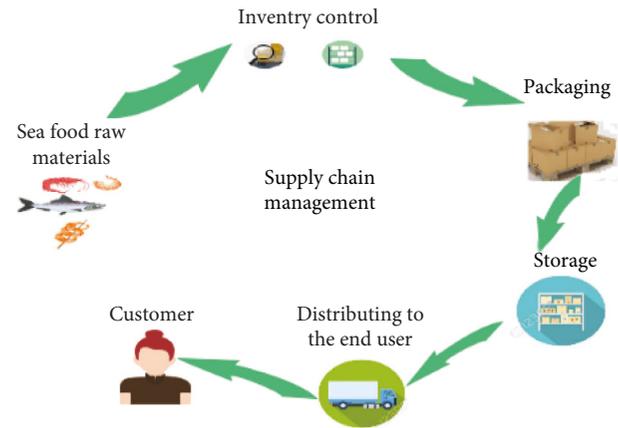

FIGURE 1: Sea food supply chain management.

to leverage the block chain's immutability in a scalable manner. The overall scheme introduces a distributed edge-based SCM network where the data is uploaded to the blockchain based on its priority. Table 1 shows the input data and their notations that were processed by edge nodes.

The architectural flow of the proposed scheme consists of an access network where each edge node is coupled with IoT sensors meant for tracing location, temperature, and humidity levels. The location information of the vehicles is traced using RFID tags in each vehicle, and the temperature and humidity levels are measured using temperature sensors. After connecting the devices at each edge node, IP addresses for each device are returned. Then, each edge node performs broadcasting of each information over the SCM network once it receives. Next, the sharing of information is accomplished through the blockchain consensus scheme. Each edge data detects for its priority score using intelligent fuzzy K-means classification. When the IoT sensors detect the high-priority data, they will upload the corresponding information to the edge node. When the smart contract recognizes the intended information, it will then stimulate the HPSAC for secure data transfer over the SCM network. The schematic flow of the suggested methodology is illustrated in Figure 3.

4. Result and Discussion

4.1. Basic Edge-Based Blockchain Structure. Due to the technological advances in blockchain, numerous applications have adopted blockchain as their business strategy. Some of the noteworthy footprints of blockchain are Bitcoin, Ethereum, and Hyperledger platforms. Bitcoin and Ethereum platforms generally adopt the Proof of Work Consensus mechanism with high-end security, but it needs more energy and computation power. On the other hand, Hyperledger uses the Byzantine fault tolerance to secure the blocks. It often relies on the number of failure nodes while securing the network. The number of failure nodes should not exceed one-third part of the available nodes. In Sybil attacks, the Hyperledger network is cumbersome as most of the nodes become compromised by the attackers, which damages the whole framework. Recent applications have adopted
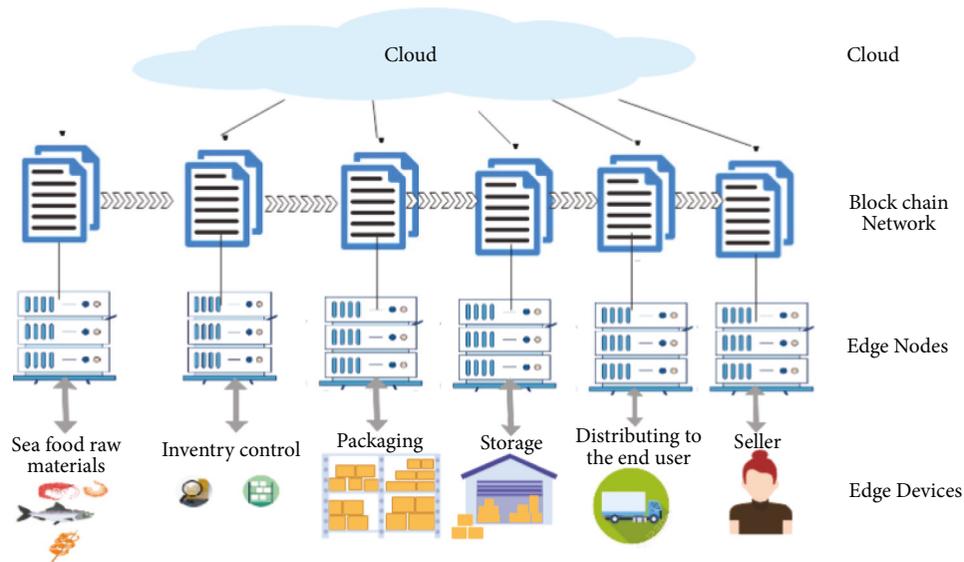
FIGURE 2: System architecture.

TABLE 1: List of inputs processed in edge nodes.

Input data	Notation
Name of the manufacturer	N_1
Name of the manufacturer company	C_1
Name of the manufacturer city	P_1
Manufacturer contact number	M_1
Name of the truck company	N_2
Name of the truck dealer	N_3
Name of the truck dealer city	P_2
Truck dealer contact number	M_2
Logistics company name	N_4
Name of the logistics dealer name	N_5
Logistics dealer contact number	M_3
Time and date of delivery of raw sea food to the manufacturer	TD_1
Temperature recorded at the time of arrival of sea foods in raw state	T_1
Time and date when the sea food taken by the distributors	TD_2
Temperature of the sea food recorded while reaching the distributors end	T_2
Time and date when the sea food loaded in the center	TD_3
Temperature of the food in the logistics section	T_3
Time and date when the sea food transported from the logistics section to the shipment truck	TD_4
Temperature recorded at the truck	T_4
Time and date when the sea food gets loaded to the retailer end	TD_5
Temperature of the food at the retailer section	T_5
Time and date when picked up by the consumer	TD_6
Temperature of the sea food at the time of arrival	T_6
Customer name	N_6
Customer contact number	M_4
Customer city	P_3

Ethereum for its feature of adopting Proof of Stack (PoS). It consumes less energy and resource and thereby increasing the scalability of the network. Moreover, Hyperledger possesses constraints such as configuring sandbox and uncertainty, directly affecting the system's security.

Henceforth, we decide to use Ethereum as the blockchain platform for its enhanced reliability and scalability. The proposed edge-based blockchain architecture is shown in Figure 4. The bottom layer consists of data that are gathered from the IoT devices connected across the SCM networks. As stated in Table 1, each edge node collects the information about the status of sea food at each instance. Next, the blockchain layer enables the key enabling features such as distributed networking, disseminating the data across the network, and verification of prioritized data among all the edge nodes. The PoS layer constitutes the sharing of data
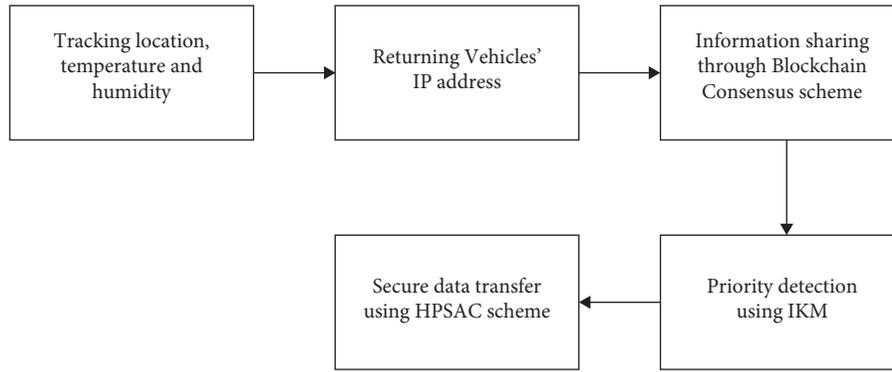
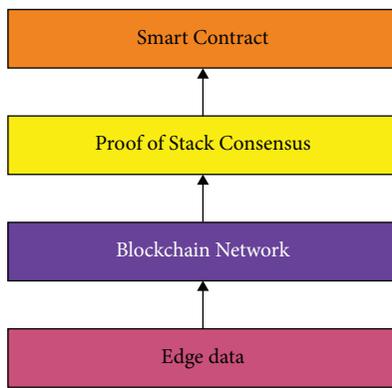FIGURE 3: Overall process flow of the proposed system.

FIGURE 4: Structure of edge-based blockchain.

among the edge nodes by adopting PoS Consensus mechanism. The smart contract layer performs the HPASC scheme for real-time secure access of the SCM network.

4.2. Priority Detection Using Intelligent K-Means (IKM) Algorithm. Consider a scenario; the seafood is produced in the manufacturer factory, the IoT sensors and RFID measure the temperature and location information, and the corresponding data are stored in the manufacturer edge servers. Likewise, the sensors continuously transmit the data gathered at different instances such as inventory, packaging, storage, distribution, and the retailer section. The data are gathered in the edges manipulated for analyzing the priority of each data before uploading to the blockchain. An example of the sensor messages gathered at the manufacturer end is a 3-tuple data: <*Timestamp*, *Sensor ID*, *content*>.

Furthermore, RFID tracks the location of the food material transported across the path. The dataset consists of additional information stated in Table 1. In our proposed scheme, priority detection is the primary step. The detection mechanism includes the intelligent k-means algorithm for detecting the priority of the data. This section furnishes the principle of IKM and IKM process.

4.2.1. Principle of IKM. Clustering mainly leads to data partition into various clusters to find out the closest relationship between those data objects. In this context, we plan

TABLE 2: Attributes and weights.

Attribute	Relative preference weight
N_1	0.2
C_1	0.2
P_1	0
M_1	0.6
N_2	0
N_3	0.2
P_2	0.5
M_2	0.6
N_4	0.4
N_5	0.5
M_3	0.3
T_6	0.91
M_4	0.4
TD_1	0.96
T_1	0.98
TD_2	0.96
T_2	0.93
TD_3	0.91
T_3	0.93
TD_4	0.94
T_4	0.96
TD_5	0.94
T_5	0.92
TD_6	0.91
N_6	0.3
P_3	0.2

to propose a massive-scale prioritization using Intelligent K-Means (IKM) in which the number of clusters and attributes are massive. In this research, we perform clustering based on the stakeholders' requirements such as food condition tracked by IoT sensors and time and date at each instance from shipment to delivery. At the outset, the preferential requirements from stake holders are selected before implementation. Then, normalized weights for each attribute are calculated accordingly. In this scenario, the requirements set of all attributes are collected from 5 stack holders. The preferential requirements lie in the range (0, 10).

Upon collecting the preferential requirements from the stack holders, the relative weights for each attribute are being calculated for scaling the value between 0 and 1. The normalized weights are computed using the following equation:
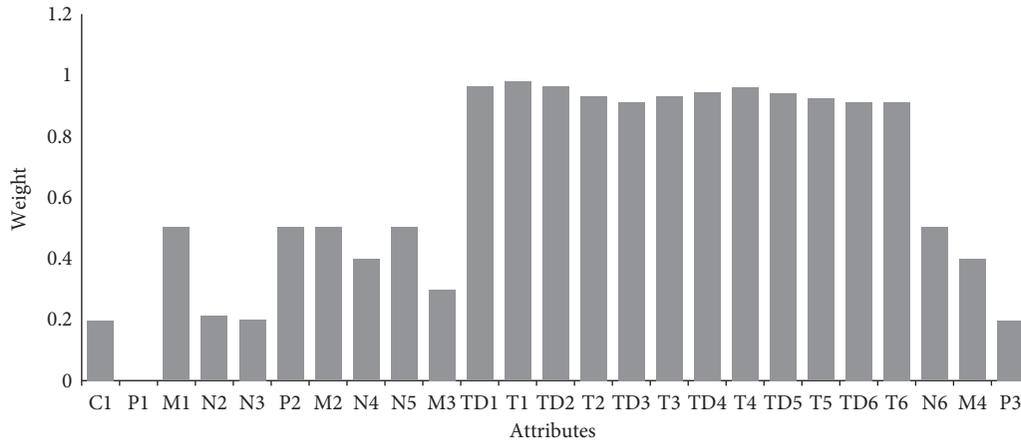
Figure 5: Illustration of weights and attributes.

$$X_{\text{normalized}} = \frac{X - X_{\min}}{X_{\max} - X_{\min}}. \tag{1}$$

For example, the average value of $N_1 = 1.2$, the minimum value of X is 1, and the maximum value of X is 2. Hence, by using (1), the normalized value of $N_1 = 0.2$.

Generally, the preference weights for temperature and time & date will be high when compared to other information stored in the edge servers. Hence the weights for each attribute are illustrated in Table 2. It clearly shows that the weight of attribute T_1 is higher when compared to other attributes.

In Figure 5 the bar graph shows the relative weights of the given attributes. K-means clustering is an unsupervised learning model that allows the realization of similar data in clusters. We adopted k-means to effectively segregate the attributes into two clusters ($K = 3$) based on the priority of each attribute. The primary objective of the k-means is to find similar groups or assign the preferential weights to the cluster based on the similitude among the attributes. Some of the basic terminologies involved in K-means are as follows.

Cluster: It is the grouping of identical data points having some similarities among each other and being accumulated.

Centroid: Random data point assumed as the center of the cluster made.

K- parameter: It refers to the target variable that denotes the number of centroids (clusters) in the corresponding dataset. Here, k denotes the number of clusters.

Mean: It refers to the average of data points for calculating the centroid in the cluster.

Euclidean distance: It is defined as the root-mean square of the addition of squared distances between the two points. Let $P(x_1, x_2)$ and $Q(y_1, y_2)$, then ED is given by

$$ED = \sqrt{(x_1 - y_1)^2 + (x_1 - y_1)^2}. \tag{2}$$

And the general form of (2) is given in the following equation:

$$ED = \sqrt{\sum_{i=1}^{n} (x_i - y_i)^2}. \tag{3}$$

4.2.2. IKM Process. This section clearly depicts the process flow of IKM. For efficient clustering of data, each edge node performs clustering of data with its relative weights. It consists of following steps.

Step 1: First, select the attributes and weights stored in each edge.

Step 2: Calculate the preferred relative weights for each attribute.

Step 3: Scale the weights for each attribute to the range 0 to 1.

Step 4: Scatter the points in the two-dimensional space to perform clustering.

Step 5: Select the 'k' value. Consider in this case $k = 3$.

Step 6: Pick random points in the cluster and consider those points as the centroid.

Step 7: Distance from the first point to the chosen centroids has to be identified.

Step 8: Calculate the Euclidean distance (ED) using equation (2). If the measured ED from the first point to the first centroid is minimum, then consider the first point to be in the first cluster. If the measured ED from the first point to the second centroid is minimum, then the first point belongs to the centroid II. Likewise, the ED for first data point to the third centroid is measured and if this distance is minimum, then the first data point belongs to the third cluster.

Step 9: Updating centroids for every arrival of new data point has to be ascertained using equation (4). The vectorized value of the centroid has been calculated as
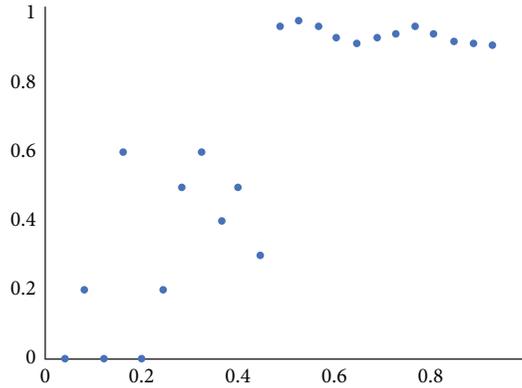
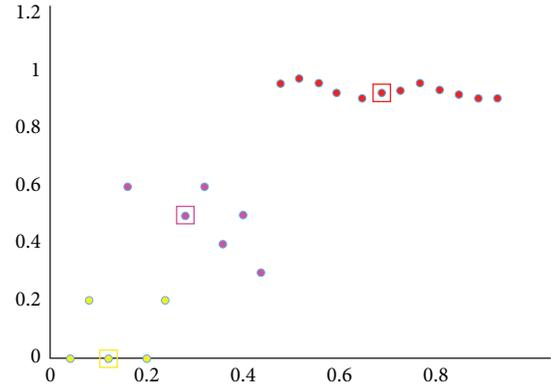FIGURE 6: Scatterplot of the preferred relative weights.

FIGURE 7: Clustering of data points after iterations with $k = 3$.

TABLE 3: Attributes with cluster value.

Attribute	Relative preference weight	Cluster
N_1	0.2	1
C_1	0.2	1
P_1	0	1
M_1	0.6	2
N_2	0	1
N_3	0.2	1
P_2	0.5	2
M_2	0.6	2
N_4	0.4	1
N_5	0.5	2
M_3	0.3	1
T_6	0.91	3
M_4	0.4	2
TD_1	0.96	3
T_1	0.98	3
TD_2	0.96	3
T_2	0.93	3
TD_3	0.91	3
T_3	0.93	3
TD_4	0.94	3
T_4	0.96	3
TD_5	0.94	3
T_5	0.92	3
TD_6	0.91	3
N_6	0.3	2
P_3	0.2	1

TABLE 4: Attributes with priority label.

Attribute	Priority Label
N_1	Low
C_1	Low
P_1	Low
M_1	Medium
N_2	Low
N_3	Low
P_2	Medium
M_2	Medium
N_4	Low
N_5	Medium
M_3	Low
T_6	High
M_4	Medium
TD_1	High
T_1	High
TD_2	High
T_2	High
TD_3	High
T_3	High
TD_4	High
T_4	High
TD_5	High
T_5	High
TD_6	High
N_6	Medium
P_3	Low

$$V_{\text{centriod}} = \frac{1}{|\text{centriod}_i|} \sum_{j=1}^{\text{centriod}_i} x_j. \tag{4}$$

Step 10: Repeat the step 7 to all the attributes with its preferred relative weights.

Figure 6 represents the scatterplot of the preferred relative weights and Table 3 illustrates the attributes and its corresponding clusters. Simply bringing the total beta weights for each person's judgement up to 100 yields the relative weights. As combined with beta weights, relative weights will always be positive.

Using Table 3, the raw values are plotted in the scattered plot, followed by choosing the number of clusters $k = 3$.

Then, by assigning the random centroid and calculating the similarity, the centroids are getting updated and final clusters are ascertained. The process of clustering involves grouping the population or data points into a number of groups such that the data points within each group are more similar to one another than the data points within other groups. Simply said, the goal is to separate groups with similar characteristics and place them in clusters. Figure 7 depicts the clustering of data points with $k = 3$. The red square box indicates the centroid point of cluster 3, which normally holds the high-prioritized data. The purple box indicates the centroid point of cluster 2 having medium-prioritized data, and the yellow square indicates the centroid of cluster 1 having low-prioritized data. Finally, Table 4

illustrates the priority label as low, medium and high according to each attributes.

The proposed scheme encapsulates the high-prioritized data for further uploading to the blockchain by excluding the medium- and low-prioritized data. The low- and medium-prioritized data remain in the edge storage for further analysis. After exempting the low- and medium-priority data, the data set is reformed, in order to reduce the block size. Eventually, it enhances the scalability in the entire blockchain network.

4.3. High Priority-Access Based Smart Contract (HPASC).
This section highlights the terminologies and processes used in the proposed HPASC scheme. It includes Blockchain and Consensus, PoS and Smart Contracts, and implementation of high-priority access-based smart contract. To achieve scalability in the blockchain SCM network, HPASC serves the purposes like reducing the block size with PoS consensus.

4.3.1. Blockchain and Consensus.
Recent surveys have reported that blockchain databases store 10% of the global GDP per the world economic forum. Blockchain is a distributed ledger that can be operated by multiple nodes situated in different locations. Also, it is a decentralized system where each node can have the ability to create a block. Essentially, blockchain is a set of blocks that undergo a set of transactions, which creates a cryptographic hash; henceforth, if any intruder attempts to tamper with the content, the link to the previous block being lost due to the change in the hash value. In addition, there may be byzantine nodes that are malicious in some instances, trying to claim false consensus across the nodes in the blockchain. Consensus in the blockchain is the voting mechanism given for a new node to get accepted as a block in the network. It is a set of transactions that becomes a part of the ledger with a common notion, "the neutral nodes are voting all blocks in the network."

4.3.2. Proof of Stack (PoS) and Smart Contracts.
In the proposed scheme, we took Ethereum blockchain to perform supply chain management. The consensus algorithm considered here is the Proof of Stake, which performs the consensus with a limited resource. Consensus is sometimes proof of stake in which a miner puts a stake by claiming itself as a voter with a certain percentage of voting rights. If a node votes for a malicious node, then it loses its stake. Before a node claims to become part of the blockchain, it allows putting a stake over the intended blockchain network. Henceforth, a node with the highest stack won the puzzle and become a part of the blockchain network. In the Ethereum network, trust is built by running smart contracts for every transaction. For instance, if the supplier needs to sell their product for $100, the buyer also accepts the product cost and accepts the order for payment with commission cost for the delivery company. The smart contract is an automated system that consists of a plan of codes working under **if-then rules**.

Figure 8 shows the smart contract in supply chain management. The figure illustrates that the manufacturer can gain the profit only if the end user receives the product and the supplier can receive the money if the buyer receives the product and the delivery company can receive the commission only if they successfully deliver the product.

4.3.3. Implementation of HPASC.
Our proposed HPASC adopts a PoS consensus mechanism for sharing the information among the nodes. When the edge node E includes a new transaction consisting of attributes stated in Table 1, the adjacent edge node will obtain the transaction details. The edge node labels the attribute with its priority values and stores the data in the blockchain through the high-priority access-based smart contract. When the next edge nodes start receiving the recently added transaction, which was broadcasted by the edge node E, it then verifies the device IP addresses and data format of the transaction. After the completion of the verification process, the other edge nodes update the information through the high-priority access-based smart contract. The HPASC Algorithm 1 is illustrated below.

The prioritization of the attributes is realized by implementing the HPASC scheme over the edge servers without the intervention of untrusted third parties. Every HPASC includes the following activities.

(i) The HPASC scheme inquires the attribute information from the edge nodes and obtains the priority value of each attribute that are about to pass through the information of the prioritized attributes.

(ii) According to Algorithm 1, the priority information submitted by edge nodes is formulated by using the HPASC scheme. Henceforth, the HPASC scheme forecasts the prioritized information to the corresponding edge nodes. Once the edge nodes receive the information, it updates in its blocks for further processing.

In HPASC, the incoming attributes are trained using the improved K-means algorithm for classifying the attributes with its priority labels. IKM is used to detect each weight as discussed in Section 1.1. If the incoming attribute contains the prioritized attribute, the HPASC scheme gets triggered. According to Algorithm 1, the HPASC scheme sends the high-priority attributes to the edge nodes. After the edge nodes pass the information finely, the edge nodes upload the information to the block, and storing the remaining information in the local storage buffer.

The rise of blockchain technologies starts increasing in growing numbers but still, the scalability challenges the network's performance. The block size for storing the data is limited to 1 MB [24]. In recent scenarios, the reduced block size has become the biggest bottleneck. Nowadays, blockchain is facing raise in waiting time per transaction due to the limited block size and generation of forks for every
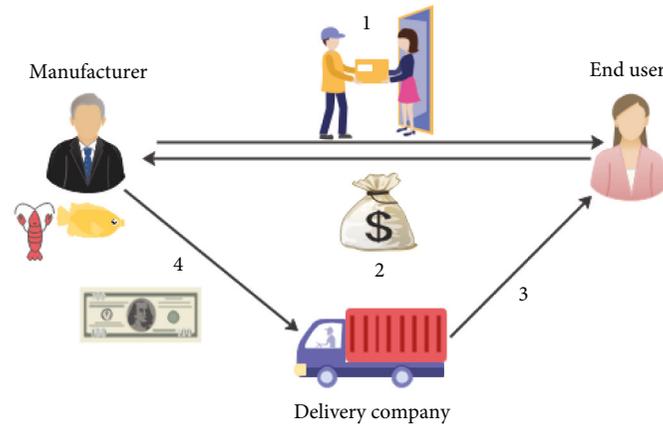
FIGURE 8: Smart contract in supply chain management.

Input: Attribute Information and Device ID
Output: High Prioritized Information in the blocks
Information_for_Sharing//Every edge node uploads the information to be stored in blockchain
Prioritized_attribute_dataset//data set having prioritized information
Edge_storagebuffer//data set having information for future analysis
Information_for_localstorage //Every edge node stores the information in local storage
P//Whether the attribute labelled with priority = 'high'
if **P** then
        Prioritized_attributedataset.add (Information_for_sharing) //Upload theimportant information to the blockchain
else
        Edge_storagebuffer.add (Information_for_local storage) //Stores the information in local storage buffer
endif
return Information_for_Sharing

ALGORITHM 1: High-priority based access based smart contract.

transaction. As a result, the time taken for block generation also increases exponentially with poor throughput.

Furthermore, the transaction constitutes transaction cost which becomes a great burden for micro-industries. Finally, the proliferation of blocks leads to high memory consumption. More generally, the scalability problems are classified into two main categories.

  (i) Storage space

(ii) Waiting time

The major objective of performance evaluation is to validate how the proposed scheme provides scalability to the SCM blockchain users. Three existing schemes, such as Chain Partitioning [24], DAG scheme [21], and Horizontal Scalability mechanism [22], are taken into consideration and compared with the proposed HPASC scheme.

Consumed stores essentially refer to the use of consumables. Sports equipment, for instance, is consumable at a club. Magazines are a consumable in a library. The act of storing goods in warehouses and logistical facilities is known as storage. Its function is to keep the market supplied with products on a consistent basis to bridge the temporal gap

between producers and consumers. From the implementation results, the comparison is made between the number of transactions and the scalability parameters, which is illustrated in Figures 9 and 10. First, a comparison is made between the number of transactions and block size to analyze the storage efficiency. Initially, we start investigating the effect of the Ethereum platform on applying the existing scalability solutions and HPASC.

For analysis, we gradually increase the transaction from 16 to 2048 transactions and analyze the impact on the count of successful transactions over the entire run of 90 transactions. The storage space occupied by every transaction is being recorded and tabulated in Table 5. The proposed scheme reports reduced storage consumption when compared to the existing mechanisms.

It is observed in Figure 9 that the consumption of storage by the blocks eventually is less in HPASC when compared to different transactions [20–22].

Furthermore, the average waiting time for every transaction is being recorded and tabulated in Table 6. In Ethereum Blockchain platforms, every transaction has to be verified before it is mined. Hence the increase in network
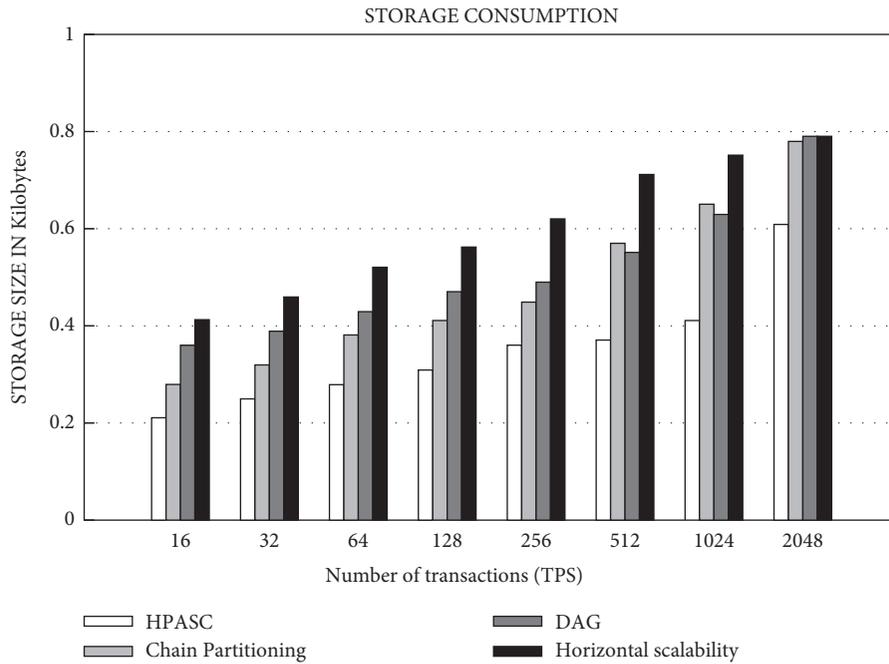
STORAGE CONSUMPTION

FIGURE 9: Storage consumption graph.
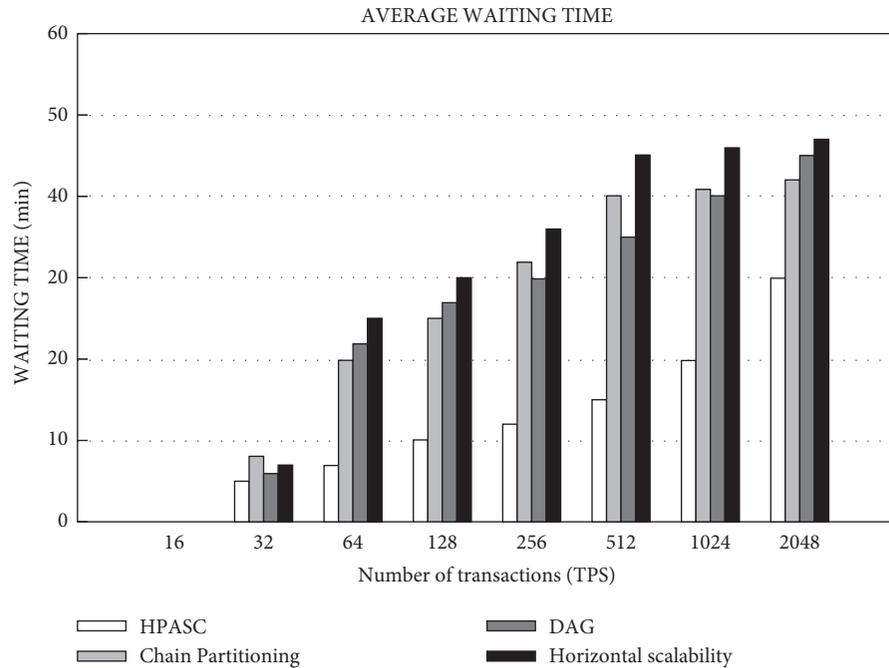
AVERAGE WAITING TIME

FIGURE 10: Average waiting time graph.

size may lead to an increase in verification time. Furthermore, it results in the elevation of waiting time due to the increase in queue size in the blocks.

From Figure 10, the average waiting time for handling the transactions found to be less in the HPASC scheme when compared to the other existing scalability solutions. Average Waiting Time is often known as A.W.T. The

average amount of time a call spends in the queue before an agent responds is known as the Average Speed of Answer (ASA). Since this is the typical wait time that callers encounter, it is also referred to as the "Average Delay". The measure is accessible per ring group, per number, and for the global account. Hence, the proposed scheme effectively overcomes the scalability challenges by

TABLE 5: Storage size for every transaction.

Transactions (block size)	Storage space in KB			
	HPASC	CPM	DAG	HSM
16	0.21	0.28	0.36	0.41
32	0.25	0.32	0.39	0.46
64	0.28	0.38	0.43	0.52
128	0.31	0.41	0.47	0.56
256	0.36	0.45	0.49	0.62
512	0.37	0.57	0.55	0.71
1024	0.41	0.65	0.63	0.75
2048	0.61	0.78	0.79	0.79

TABLE 6: Waiting time for 2048 transactions.

Transactions (block size)	Average waiting time in mins			
	HPASC	CPM	DAG	HSM
16	0	0	0	0
32	5	8	6	7
64	7	20	22	25
128	10	25	27	30
256	12	32	30	36
512	15	40	35	45
1024	20	50	40	46
2048	30	55	45	47

TABLE 7: Simulation parameters.

Max transactions per block	10
Maximum block generation time	30 s
Consensus algorithm execution time	200 ms
Transaction generation rates	[10, 40, 100] txs/s
Transaction generation rates changing time	[2500, 4000] s

uploading high -prioritized information to the blocks. Table 7 depicts the simulation parameters.

5. Conclusion

An HPASC scheme is applied to achieve scalability in blockchain-based SCM networks. Experimental results report that the priority classification using intelligent k-means clustering over the supply chain datasets works effectively and feasibly. Later, Ethereum was taken as the underlying blockchain platform to carry out the consensus mechanism over the edge networks. Three existing methods are considered and compared to the proposed HPASC scheme, including Chain Partitioning, DAG scheme, and Horizontal Scalability Mechanism. By accurately identifying the properties in the data set, the proposed method primarily improves the scalability of the edge-based blockchain. Comparison results show that the selected scheme reports good scalability against some existing mechanisms. As further work, the real-time datasets can be used to perform relevant operations to achieve scalability in the supply chain networks.

There are new potential to improve supply chain integrity and operational effectiveness when blockchain technology is combined with IoT. As a result, new issues may arise as a result of the new technology. The immutability of a blockchain, for example, is viewed as a crucial property. Many factors have sparked increased interest in the creation of "mutable" blockchains, but immutability is one of them. As a result, more academic study is required to thoroughly investigate, explain, and forecast various application situations. It is vital to keep in mind that blockchain integration in an IoT setting has a number of restrictions and obstacles. As IoT infrastructure grows in complexity, the blockchain will be at the forefront of handling ever-increasing volumes of data that demand very high scalability. Permissioned blockchains, which are less resource-intensive, may help with privacy and scalability concerns, and the idea of "Blockchain pruning" has been floated as a potential solution. Although these alternatives feed the debate over Blockchain's immutability and the monopolistic attitude of consortium ledgers, which imposes obstacles to entry and inhibits innovation, these alternatives are still a viable option.

Data Availability

The data that support the findings of this study are available on request from the corresponding author.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

References

[1] B. Lester, "Best Supply Chain Blockchain Projects, Rated and Reviewed for 2019," 2019, https://www.remedi.com/blog/best-supply-chain-blockchain-projects-rated-and-reviewed-for-2019.

[2] R. Krishnamoorthi, S. Joshi, H. Z. Almarzouki et al., "A novel diabetes healthcare disease prediction framework using machine learning techniques," *Journal of Healthcare Engineering*, vol. 2022, Article ID 1684017, 10 pages, 2022.

[3] A. Rizwan, P. Priyanga, E. H. Abualsaud, S. N. Zafrullah, S. H. Serbaya, and A. Halifa, "A Machine Learning Approach for the Detection of QRS Complexes in Electrocardiogram (ECG) Using Discrete Wavelet Transform (DWT) Algorithm," *Computational Intelligence and Neuroscience*, vol. 2022, Article ID 9023478, 8 pages, 2022.

[4] N. Alzahrani and N. Bulusu, "Block-supply chain: A new anticounterfeiting supply chain using NFC and blockchain," in *Proceedings of the CRYBLOCK 2018 - 1st Work. Cryptocurrencies Blockchains Distrib. Syst. Part MobiSys*, pp. 30–35, ACM, Munich, Germany, June 2018.

[5] N. Kefalakis, N. Leontiadis, J. Soldatos, K. Gama, and D. Donsez, "Supply chain management and NFC picking demonstrations using the AspireRfid middleware platform," in *Proceedings of the ACM/IFIP/USENIX Middlew. 2008 Conf. Companion*, pp. 66–69, ACM, Leuven, Belgium, December 2008.

[6] O. K. Ha, Y. S. Song, K. Y. Chung, K. D. Lee, and D. Park, "Relation model describing the effects of introducing RFID in the supply chain: Evidence from the food and beverage

industry in South Korea," *Personal and Ubiquitous Computing*, vol. 18, no. 3, pp. 553–561, 2014.

[7] Y. P. Tsang, K. L. Choy, C. H. Wu, G. T. S. Ho, and H. Y. Lam, "Blockchain-driven IoT for food traceability with an integrated consensus mechanism," *IEEE Access*, vol. 7, Article ID 129000, 2019.

[8] M. Q. Saeed, Z. Bilal, and C. D. Walter, "An NFC based consumer-level counterfeit detection framework," in *Proceedings of the 2013 11th Annu. Conf. Privacy, Secur. Trust. PST*, pp. 135–142, IEEE, Tarragona, Spain, July 2013.

[9] F. Tian, "Agri-foodchain traceability system using RFID and Blockchain," in *Proceedings of the 2016 13th International Conference on Service Systems and Service Management (ICSSSM)*, pp. 2161–1904, IEEE, Kunming, June 2016.

[10] Bo Yan and Bo Du, "Research on garment supply chain management system based on RFID," in *Proceedings of the 2009 ISECS International Colloquium on Computing, Communication, Control, and Management*, IEEE, Sanya, China, August 2009.

[11] J. L. Zhao, S. Fan, and J. Yan, "Overview of business innovations and research opportunities in blockchain and introduction to the special issue," *FinancInnov*, vol. 2, p. 28, 2016.

[12] A. Abeyratne and R. P. Monfared, "Blockchain ready manufacturing supply chain using distributed ledger," *International Journal of Renewable Energy Technology*, vol. 5, no. 9, pp. 1–10, 2016.

[13] V. Astarita, V. P. Giofrè, G. Mirabelli, and V. Solina, "A review of blockchain-based systems in transportation," *Information*, vol. 11, no. 1, 2019.

[14] A. Pradana, G. Ong, Y. Jaya, and A. A. Mohammed, "Blockchain traffic offence demerit points smart contracts: proof of work," *International Journal of Advanced Computer Science and Applications*, vol. 9, no. 11, pp. 375–382, 2018.

[15] M. A. Khan and K. Salah, "Iot security: Review, blockchain solutions, and open challenges," *Future Generation Computer Systems*, vol. 82, pp. 395–411, 2018.

[16] Y. Xiao, Y. Jia, C. Liu, X. Cheng, J. Yu, and W. Lv, "Edge computing security: state of the art and challenges," *Proceedings of the IEEE*, vol. 107, no. 8, pp. 1608–1631, 2019.

[17] S. Underwood, "Blockchain beyond bitcoin," *Communications of the ACM*, vol. 59, no. 11, pp. 15–17, 2016.

[18] I. Ahmad, S. H. Serbaya, A. Rizwan, and M. S. Mehmood, "Spectroscopic analysis for harnessing the quality and potential of gemstones for small and medium-sized enterprises (SMEs)," *Journal of Spectroscopy*, vol. 2021, pp. 1–12, 2021.

[19] H. T. Vo, Z. Wang, D. Karunamoorthy, J. Wagner, E. Abebe, and M. Mohania, "Internet of blockchains: techniques and challenges ahead," in *Proceedings of the IEEE Confs on Internet of Things, Green Computing and Communications, Cyber, Physical and Social Computing, Smart Data, Blockchain, Computer and Information Technology, Congress on Cybermatics*, IEEE, Halifax, NS, Canada, July 2018.

[20] K. Cong, Z. Ren, and J. Pouwelse, "A blockchain consensus protocol with horizontal scalability," in *Proceedings of the IFIP Networking Conference (IFIP Networking) and Workshops*, IFIP, Zurich, Switzerland, May 2018.

[21] M. Du, X. Ma, Z. Zhang, X. Wang, and Q. Chen, "A review on consensus algorithm of blockchain," in *Proceedings of the 2017 IEEE International Conference on Systems, Man, and Cybernetics (SMC)*, pp. 2567–2572, IEEE, Banff, AB, Canada, Oct. 2017.

[22] S. Mondal, K. P. Wijewardena, S. Karuppuswami, N. Kriti, D. Kumar, and P. Chahal, "Blockchain inspired RFID-based information architecture for food supply chain," *IEEE Internet of Things Journal*, vol. 6, no. 3, pp. 5803–5813, 2019.

[23] J. Tu and S. Piramuthu, "On Addressing RFID/NFC-based relay Attacks: An overview," *Decision Support Systems*, vol. 129, no. 2, Article ID 113194, 2019.

[24] Q. Zhou, H. Huang, Z. Zheng, and J. Bian, "Solutions to scalability of blockchain: A survey," *IEEE Access*, vol. 8, Article ID 16440, 2020.