sustainability

MDPI

Article

Privacy-Preserving Blockchain Framework for Supply Chain Management: Perceptive Craving Game Search Optimization (PCGSO)

Basim Aljabhan [1] and Muath A. Obaidat [2,*]

[1] Ports and Maritime Transportation Department, Faculty of Maritime Studies, King Abdulaziz University, Jeddah 21589, Saudi Arabia
[2] Department of Computer Science and Information Security, City University of New York, New York, NY 10019, USA
* Correspondence: muobaidat@ccny.cuny.edu

Abstract: The fierce competition in international markets and the rapid advancements in information technology result in shorter lead times, lower transportation capacity, and higher demand. The supply chain network is one of the most crucial areas of concentration in the majority of business circumstances. Blockchain technology is a promising option for safe information exchange in the supply chain network. Although preserving security at every level of the blockchain is somewhat important, cryptographic methodologies are frequently used in the existing works. The novel perceptive craving game search (PCGS) optimization algorithm is used to optimally generate the key for data sanitization, which assures the privacy of logistics data. Here, the original logistics data obtained from the manufacturer is sanitized with an optimal key generated by using the PCGS optimization algorithm, avoiding the risk of unauthorized access and data swarm that causes the system to lag. Moreover, the sanitized data obtained from the manufacturer is transmitted to the allowed parties via different sub-chains. The same generated key is used on the receiving customer side for reconstructing the original information from the sanitized data. The performance and results of the proposed blockchain-based privacy preservation model are validated using various parameters.

Keywords: supply chain management (SCM); logistics; blockchain; privacy preservation; security; key generation; perceptive craving game search (PCGS) optimization algorithm

check for updates

Citation: Aljabhan, B.; Obaidat, M.A. Privacy-Preserving Blockchain Framework for Supply Chain Management: Perceptive Craving Game Search Optimization (PCGSO). *Sustainability* **2023**, *15*, 6905. https://doi.org/10.3390/su15086905

Academic Editor: Giada La Scalia

Received: 24 February 2023
Revised: 8 April 2023
Accepted: 13 April 2023
Published: 19 April 2023

Copyright: © 2023 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

1. Introduction

The supply chain [1,2] is defined as a type of network used mainly in industrial sectors for satisfying customers according to their requirements. This framework encompasses the producers, wholesalers, retailers, customers, and traders. Similarly, supply chain management [3–5] is mainly developed for strategically managing the marketing channels, storage materials, components, and procurement for enhancing future profitable growth. The intricate production and distribution of items are both a part of the supply chain. It has a variety of stages, geographical locations, accounts, and payment methods, as well as a number of people, organizations, and modes of transportation, all depending on the product. As a result, the supply acquisition process can take many months [6]. The stakeholders in the logistics process are very interested in introducing and developing blockchain technology to improve the logistics operations in the supply chain [7,8] and make them economically sustainable because of the complexity and lack of transparency inherent in logistics. The most common uses of blockchain technology are in cryptocurrencies, although there is a much wider range of potential applications [9]. A distributed book (ledger) called blockchain [10,11] has a wide range of possible uses. Any data interchange, including contract negotiations, product tracking, and financial transactions, can be conducted with it. The system is transparent, since each activity is recorded in the

block and the data is dispersed among numerous nodes. The system is safe, since each block is connected to the one before it and the one after it [12]. Blockchain technology has the potential to improve all logistical procedures, including storage, transport, and payment, as well as the efficiency and transparency of the supply chain [13]. With blockchain, it is possible to speed up the physical flow of commodities while achieving improved security [14,15] and transparency. The blockchain-based tracking [16] of items can enhance decision making, which will ultimately lead to more satisfactory service for the customer. The literature [17] suggests that new business models and logistics services could be developed using blockchain technology. Blockchain is a relatively new technology that aims to provide decentralization, real-time peer-to-peer operation, privacy, openness, transience, and integrity in a broadly used manner [18]. However, there are still issues and problems with this technology that must be taken into consideration. Its performance is one of the obvious drawbacks [19,20]. It will take a lot longer to verify every transaction using the blockchain method than using the centralized method because each node in the network must acknowledge it. The foundation of blockchain technology is a technique that enables previously unidentified people to collaboratively create and maintain almost any database on a fully distributed basis, with transaction integrity and completeness being verified by the consensus of teh identifiers [21–23]. In comparison to other communication platforms, blockchain has three significant advantages:

- The communication parties have unrestricted access to it and can join for free.
- Data that has been submitted cannot be changed, and in particular, the integrity assurances are not made by a centralized authority, but rather by the network as a whole.
- The published information can indeed be changed; therefore, no one can censor information that has already been made public.

As a result of the immutability of the blockchain [24], it is practically impossible to change the covert messages, and the incorporation of hidden information can be unstable. The supply chain is a collection of businesses that are connected through various processes and activities to create value in the form of goods and services for the eventual user. For several reasons, blockchains [25] are thought to be well-suited for use in the logistics and supply chain management industries. The data generated at each stage of the product's lifecycle as it moves down the value chain can be recorded as a transaction, giving the product a permanent history [26]. Blockchain is a decentralized, global ledger that is digitally managed and used to store transactions in an unchangeable way. It pertains to applications involving transactions because of its ample delivery of confidence, openness, and provenance [27]. Even non-financial industries, such as healthcare, production, retailing, and public services, have begun to take notice of the technology, which was initially developed to assist in financial transactions. However, the adoption of blockchain in SCM [28,29] is still in the development stage, and it faces many obstacles before it can provide a high level of security. For solving this problem, several new optimization algorithms have recently been developed. To maintain a high level of security [30], only a certain number of transactions can be handled in a small amount of time. In light of this, it is now difficult to balance the factors of security and block size in SCM [31,32]. Additionally, the integration of financial information in blockchain-based SCM can result in less transparency, which raises costs and lowers performance. Therefore, the proposed work [33] aims to develop a new and successful blockchain-based privacy preservation framework for SCM.

Motivation

The major contributions and objectives of this work are as follows:

- The lightweight blockchain technology-based supply chain network is modeled for enabling a secured and reliable information sharing.
- For ensuring the privacy of original manufacturer's data, an optimization-based privacy preservation technique is deployed, which includes the operations of data sanitization and data restoration.

- The perceptive craving game search optimization (PCGSO) algorithm is employed to optimally generate the key for data sanitization and restoration operations, ensuring the security and privacy of logistics data.
- The analytical results are validated and compared using various parameters for demonstrating the efficacy of the proposed privacy preservation model.

The following units make up the remaining sections of this article: Section 2 provides a complete literature review regarding the impacts of using blockchain technology for improving supply chain management in industrial sectors. The proposed blockchain-based privacy preservation framework used in the SCM system is explained in detail in Section 3 of the manuscript. By employing various factors, Section 4 validates the analytical findings of the existing and proposed blockchain models. In Section 5, the overall summary of the paper is offered, along with suggestions for further research.

2. Literature Survey

This section presents the literature review of the existing works relevant to the impacts of using blockchain technology for improving the privacy preservation of supply chain management systems. Moreover, it discusses several optimization algorithms that are currently used in the field of SCM.

Tijan et al. [34] developed a decentralized data storage system with the use of blockchain technology for supply chain management. Here, the basic properties of using blockchain have been discussed, along with its applications and uses. Typically, ensuring the transparency of supply chain management is one of the most important aspects of logistics. Raja shanthi et al. [35] provided a detailed overview of the importance of using blockchain for addressing the challenges and key issues in logistics. Specifically, a private blockchain is more suitable for multi-organizations for improving their security. The supply chain, on the other hand, is thought of as the beating heart of organizations because it ensures that goods are transported without interruption from one production process to another until they reach the customer. Pournader et al. [36] presented a comprehensive review for analyzing the major impacts of SCM in organizational sectors. The different areas covered in this work are as follows: supply management, demand management, product management, and information management. In addition to this, it investigated various risk factor associated with the SCM, which include industrial risks, problem-specific risks, environmental risks, financial flow risks, material flow risks, and decision-making risks. Ref. [37] investigated the different types of security challenges, with appropriate solutions, for IoT systems.

Gurtu et al. [38] presented a comprehensive study of supply chain risk management, along with risk management strategies. Typically, the supply chain is considered the backbone of the global economy, which supports enhancing trade and optimization of resource consumption. Heidari et al. [39] deployed a fuzzy analytic hierarchy (FAH) incorporated with the fuzzy TOPSIS model for resolving risks in the SCM. The key factor of this work was to develop a new hierarchical framework for enhancing the performance and growth of the organization, with a reduced level of risks. In this work, various processes, such as product lifestyle, operational process cycle, operational risk, and a multi-criterion decision model, were analyzed for reducing the level of risks in the organization environment. Salamai et al. [40] investigated the major impacts of internal and external factors associated with CM. The purpose of this work was to analyze the importance of deploying operational risk management strategies for the successful growth and development of the organization. Here, the different types of risk management approaches have been discussed for enhancing business growth and development. The most commonly used risk mitigation techniques in conventional works were quantitative models, arbitrary optimization techniques, theoretical models, Q-sorts analysis, and qualitative approaches.

Chang et al. [41] conducted a systematic literature review on blockchain-based supply chain management using current trends and potential applications. The authors mentioned that future orientation depends on four key issues, including procurement integration and automation, stakeholder engagement and interaction, traceability and transparency, and

shared frameworks on blockchain-based platforms. Moreover, the traditional supply chain operations involve several intermediates, problems with trust, and reduced performance. Lotfi et al. [42] introduced a new framework, called viable supply chain network design (VSCND), using blockchain technology. Here, the authors identified that crypto-currency can assist the supply chain in achieving sustainability by lowering costs and imposing versatility. Kashem et al. [43] investigated the effects of using AI and blockchain technology in supply chain management systems. The purpose of this research was to avoid supply chain interruptions with the help of blockchain and AI models. The blockchain strengthens legitimacy, privacy, and productivity in logistics while enabling reliable communication across intricate manufacturing networks. Additionally, it might create websites where transportation providers can list the trucks or ships that are currently available. Blockchain technology [44] may make it possible to create tamper-proof smart contracts for purchases that automatically uphold the conditions of cross agreements. In contrast, smart contracts can self-verify and self-execute by allocating funds to the appropriate parties. A supply chain optimization system powered by AI improves smart decisions by enhancing demand forecast with the optimal course of action. This can help manufacturers to predict the results of particular events in terms of time, expenditures, and revenue, which also helps to improve the overall performance of the supply chain. Chen et al. [45] introduced a new trusted trading framework with the use of blockchain technology. This system uses blockchain technology to create a coordination committee, and it can function without the requirement of a coordination center. Moreover, the suggested framework is immune to single-point failures due to multi-point backups. Table 1 reviews some of the existing blockchain technologies used in the conventional works for SCM.

Table 1. Survey of an existing blockchain–SCM system.

Ref.	Application Domain	Context	Technology	Model Approach
[46]	Supply chain distribution	A blockchain-based supply-chain visibility system is developed for tracking shipments in physical distribution.	Blockchain	Framework model
[47]	Smart contracts	A clear illustration is provided for determining how smart contracts are deployed in several applications that includes SCM-IoT.	IoT integrated with blockchain	Theoretical framework
[48]	Medical application system	A secured key management scheme is developed for a heterogeneous networking system.	IoT integrated blockchain model	Theoretical framework
[10]	Medical equipment SCM	A complete life cycle theory is utilized, along with blockchain technology, for the production, destruction, and traceability of medical equipment.	Blockchain	Conceptual framework
[49]	Supply chain integrity management	A blockchain-integrated SCM is deployed to enable the sharing of personal records in an accountable way for smart hospital applications.	Blockchain	Theoretical framework
[50]	Healthcare system	A blockchain-based app development allows patients to quickly exchange and control their data while also improving the security of healthcare facilities.	Blockchain	Conceptual framework

3. Materials and Methods

The complete explanation for the proposed blockchain-based privacy preservation framework for securing logistics data is presented in this section. Due to its emphasis on an industry's efficiency, SCM occupies the top priority in business enterprises. The supply chains are being connected with blockchain technology due to a lack of security

in the network. However, there is still a problem with the level of security and privacy protection. This paper develops a new blockchain-based privacy preservation framework for ensuring the security of SCM data. The main idea behind the proposed work is to develop a lightweight blockchain-based privacy preservation model for SCM. In this model, the raw logistics data obtained from the manufactures are secured with the use of a novel optimization mechanism.

Information sharing is now more feasible due to the development of information and communication technologies. The worldwide foundation of long-term coordination and collaboration has made information sharing in supply chains more effective, which has increased the competitive advantages of businesses. However, a lack of information sharing in businesses makes it difficult for organizations to effectively coordinate their efforts. The main idea behind the proposed work is to develop a lightweight blockchain-based privacy preservation model for SCM. In this model, the raw logistics data obtained from the manufactures are secured with the use of a novel optimization mechanism. This study proposed the development of a novel blockchain-based architecture for privacy preservation in the supply chain network. This work sought to improve both the security and privacy of the suggested blockchain-aided SCM, wherein the updated "data sanitization and data restoration" was carried out with an ideal key creation technique to safeguard the received data in every block. The PCGS optimization algorithm was used to select the best key, in this case.

The four primary steps of the proposed blockchain-based privacy preservation system are Layer 1–manufacturers or industries, Layer 2–entire control and management, Level 3–products or goods delivery, and Level 4–consumers (i.e., an individual or business people). In this case, key-oriented legalization certifies the validity of dependable users and grants them access to the designated data. The unrefined supplies are primarily delivered to the producers, and the blockchain is given the "raw material name, quantity, quality of material, location of the supplier. etc". The required data is then kept in the blockchain as the factory distributes the raw materials to managers of the various sectors. The commodities are then delivered to vendors by recoding the condensed data. The vendors use the blockchain to access the necessary products based on their requirements. In light of the fact that security is the primary concern in blockchain-oriented SCM, the PCGS-privacy preservation concept was developed. The blockchain has received a lot of attention from both business and academia, since it is a significant distributed and secure approach in modern business. Blockchain is described as a distributed ledger system that enables parties to move assets at a minimal cost, while securing the resolution of transactions. Here, the data sanitization and restoration processes are performed based on the key generated by using the PCGS optimization algorithm.

For analysis, the original SCM data such as the "SCMS delivery history dataset" and the "dataset of supply chains used by the company DataCo Global" have been used to validate and compare the results of the proposed blockchain-enabled PCGS privacy preservation model. Provisioning, manufacturing, sales, and corporate distribution are areas with significant registered operations that can be used with machine learning algorithms and software. In order to generate knowledge, it also permits the connection of organized and unstructured data. According to the dataset gathered, a single manufacturer developed the blockchain. The data are sent from the manufacturer (Level 1) to the managers of various nations (i.e., nations 1 and 2) through numerous sub-chains, which is through numerous sub-chains in Level 2. The data are then sent to each of the branches (Level 3) of the managing company inside each country from the manager level of each country in different sub-blocks. The feasibility of the organized job is shown by the cost function, which is a performance metric computed for testing the proposed PCGS privacy preservation model. Consequently, the other parameters, such as key sensitivity, correlation coefficient, Euclidean distance, mean, sanitization and restoration efficiency, privacy, and utility factors are also estimated and compared with the existing blockchain-enabled security models used in the SCM system. The offered work has the most secure key, making it clear from

the overall observation that unauthorized access to the material is not allowed. Moreover, the PCGS-privacy preservation was found to be better with high privacy and utility factors, when compared to the existing models; hence, it is stated that the proposed model is highly efficient for information sharing in SCM.

As shown in Figure 1, the proposed data protection scheme comprises two modules of operations: the creation of a blockchain framework for the logistics data, and privacy preservation using optimal key generation. Here, the original logistics data obtained from the manufacturer is sanitized with an optimal key generated by using the perceptive craving game search (PCGS) optimization algorithm. More specifically, there is a risk of unauthorized access and data swarm that causes the system to lag when uploading all of the cleaned data through a single blockchain. Moreover, the sanitized data from the sender is thus transmitted here to the allowed parties via different sub-chains. Sanitized data is recovered at the receiving end to retrieve the original data. The key generation, which must be carefully chosen, plays a significant role in both the sanitization and regeneration processes. Here, the key used for data sanitization is optimally generated with the help of the PCGS optimization algorithm. Due to this type of key generation and transmission operation, only authorized receivers or customers can access the logistics data, with ensured privacy.

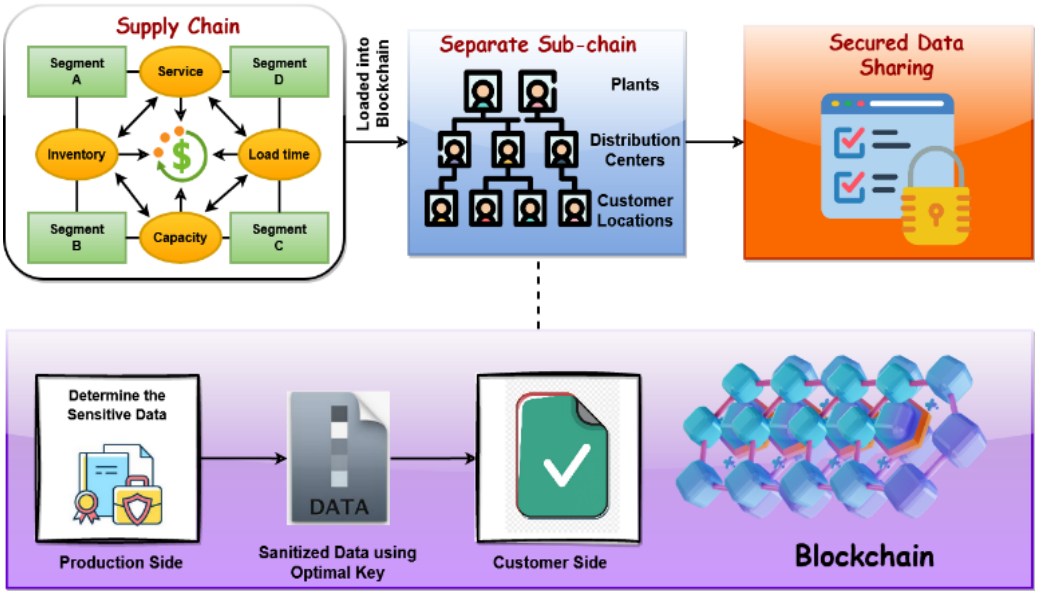

Figure 1. Overall proposed privacy-preserving blockchain framework for SCM.

First, the supply chain network is formulated, which is further loaded into the blockchain for assuring a secured logistics data transmission. Moreover, the privacy preservation mechanism has been used in the blockchain model, where the data sanitization process is performed with the help of the PCGS optimization technique. Then, the same generated key is used on the receiving customer side for reconstructing the original information from the sanitized data. The primary advantages of using the proposed blockchain-based privacy preservation are increased security, ensured data confidentiality, data validness, and less complexity.

3.1. Logistics and SCM

The logistics and supply chain support the transportation of raw materials, which are an essential component of all goods and which travel through numerous manufacturing steps to add value before being delivered to the client as a final product. The network of businesses, known as the supply chain, is connected by a variety of processes and activities that result in value being delivered to the final customer in the form of goods and services. Typically, logistics refers to the actions involved in transferring and storing

commodities between two functions within a distribution network, and the supply chain refers to the entire network of organizing, procurement, production, transportation, and delivery of products to consumers. Thus, the supply chain encompasses or includes a subset of logistics, since, extremely effective management is needed to save time and costs, with little to no waste. Managing the supply chain and logistics is also seen as one of the essential components of the product development process. The goal of supply chain management is to maintain the constant flow of goods and services by streamlining both upstream and downstream processes. The downstream supply chain refers to all actions that involve the flow of goods after manufacturing until they reach the customer, whereas the upstream supply chain refers to all activities that entail the flow of goods into the organization, from the acquisition of raw materials until the product has been produced. The layered architecture model of the proposed blockchain-based SCM framework is shown in Figure 2, which includes four distinct layers:

1. Layer 1–manufacturers or industries;
2. Layer 2–entire control and management;
3. Level 3–products or goods delivery;
4. Level 4–consumers (i.e., an individual or business people).

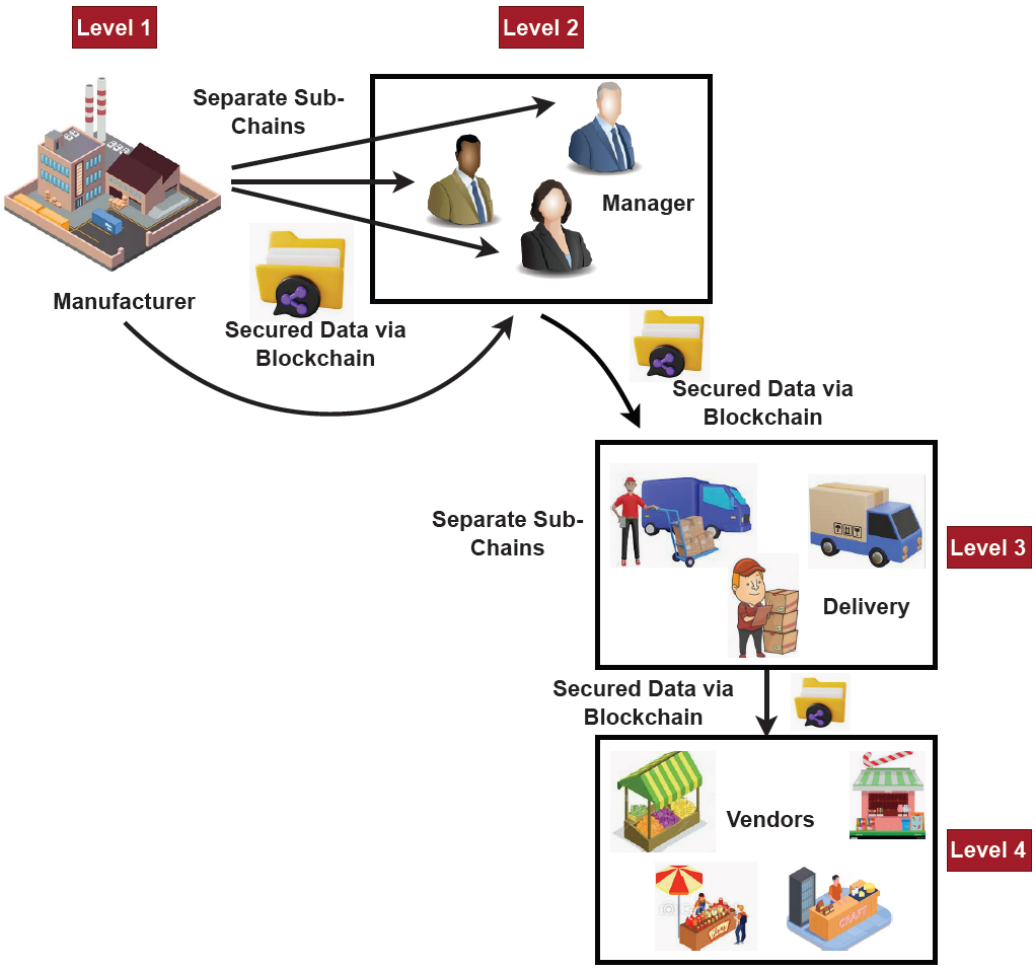

Figure 2. Layered security architecture model of the proposed framework.

In the beginning, each manufacturer in a variety of industries develops their specific database that includes information on the product they produce, its price, its quantity, the person in charge of managing the product, how it is delivered, and the details regarding the suppliers. An ideal key is used to cleanse the data produced by the manufacturers. All of this data are loaded onto the blockchain by the management. The blockchain typically consists of a sequence of blocks that surrounds the data and appears to go on forever.

Moreover, the typical structure of the block is shown in Figure 3, which comprises the fields of header, body, and transaction data. The degree of security in this situation is a critical concern to the distributed nature of the blocks. To address this issue, this research study breaks the blocks pertaining to each of the managers and delivers their relevant data in different sub-chains. As a result, this location becomes more secure. The related data are then combined into a sub-chain and sent across the supply chain network as the data is transferred from the management level to the distribution layer. The dealer level is reached via this sub-chain based information exchange. Data restoration happens on the client side. With the right key, the provider can access the original data and recover the sensitive information.

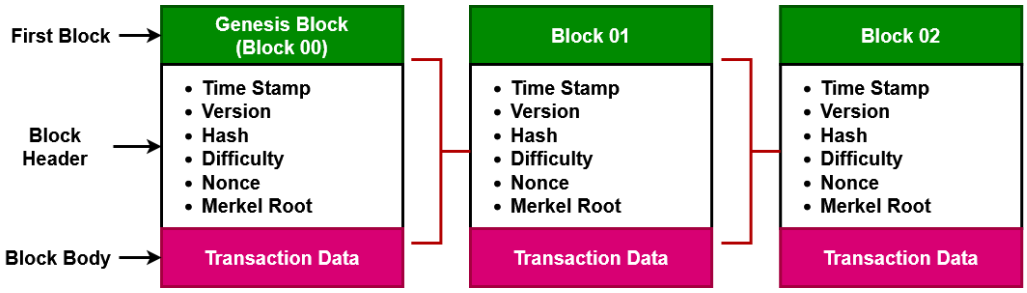

Figure 3. Structure of the block.

The layered architecture model of the blockchain enabled SCM framework is shown in Figure 2. Manufacturers frequently vary their supply chain network to include all regions of the world in order to give their customers the greatest possible user experience. Manufacturing businesses also extend their borders outside continents in order to take use of the advantages of inexpensive labor, the accessibility of materials, advantageous legislation, and a substantial customer base. Even a single weak link in the network can cause interruptions and delays in such a fiercely competitive industry, which can negatively impact customer satisfaction and have a significant impact on a company's financial performance. Each of these manufacturers develops a unique product database that comprises the information such as item description, quantity, weight, brand label, etc. The manufacturers upload their data to the blockchain, which then creates a unique sub-chain for each manager. As a result, by restricting unauthorized access to information, the security of the blockchain is increased to a greater extent. The managers typically generate their own sub-chain for the vendors by gaining access to their sub-chains.

A block of data saved in a blockchain can be thought of as a write-once, read-only database; some important data recorded in a block is shown in Figure 3. Each block is divided into a header and a body, and a hash is used to identify each block. The metadata, which includes the timestamp, version, hash value, difficulty, nonce, and Merkel root, is kept in a block header, as illustrated in Figure 3. When a block is added to the blockchain, its timestamp serves as both a reference point and verification of its addition. The used version of the blockchain is indicated by version, in which version 2.0 and 3.0 are typically used for the decentralized and smart contract application systems. Applying a cryptographic hash function to the data is the process of hashing. The fundamental building element of a blockchain network is a hash function, which transforms incoming data into a string of bytes with a predetermined length and structure. The miners are in charge of creating new blocks, and each block includes a hash that connects it to the one before it. The hash rate of the network and the number of mining nodes determine how long it would take to add a new block of the transaction to the blockchain. This value is called the difficulty. The network is more secure, and the processing power required to validate transactions increases with difficulty. A 32-bit random number, called a nonce, which stands for "number only used once", is used for identification, hashing, verification, or digital signatures. A mathematical method that condenses the transactions in a block is called a Merkle root. It checks to see if information in a Merkel tree has been altered, hacked,

or changed in any way. Business information, including the transaction counter and the transaction details, are contained in the block's body.

3.2. Privacy Preservation

Typically, data privacy can be assured in different ways with the use of encryption, perturbation, sanitization, etc. When compared to the other models, sanitization is the most suitable mechanism currently widely used for data security. In this research, a unique privacy preservation method is explored in which sensitive information is hidden from the intermediate level, which is more vulnerable to the stakeholders involved in communication, by applying the process of data sanitization and restoration. In supply chain management, material moves from level 1 to level n, from industry to industry, and secure blockchain technology is utilized to process this data. Suppliers create databases with different fields for private and sensitive information; private information must be concealed from the management and marketing agent. After a successful key generation, the key can be passed on to the authentication procedure at the producer level. Typically, data sanitization and restoration are the two main techniques that can be used to maintain data privacy. To effectively protect sensitive data during the sanitization process, a key is initially produced. It is crucial to construct the key as optimally as possible because it is produced in a way that should significantly disguise the sensitive data from adversaries. To create the ideal key, a hybrid optimization approach is used. The sanitized data can be further recovered at the receiver's end by the authenticated user using the same optimum key. In this framework, the association rules are first extracted from the source database using this method. At the manufacturer level, data gets cleaned up, and the blockchain must be cleaned up as well. Each piece of sensitive data in each sub-block of the blockchain must be sanitized, since the data is transmitted in smaller units called sub-blocks. The non-sensitive data do not change over time and do not require sanitization. In general, this is described as a data protection strategy where sensitive data is secured using the optimal key. This procedure involves first transforming the chosen key to a binary value, which is then multiplied by the original data. As a result, the acquired data is known as sanitized data and is graphically represented in Figure 4. Secured data transmission is ensured by a data sanitization procedure working in tandem with a privacy preservation strategy.

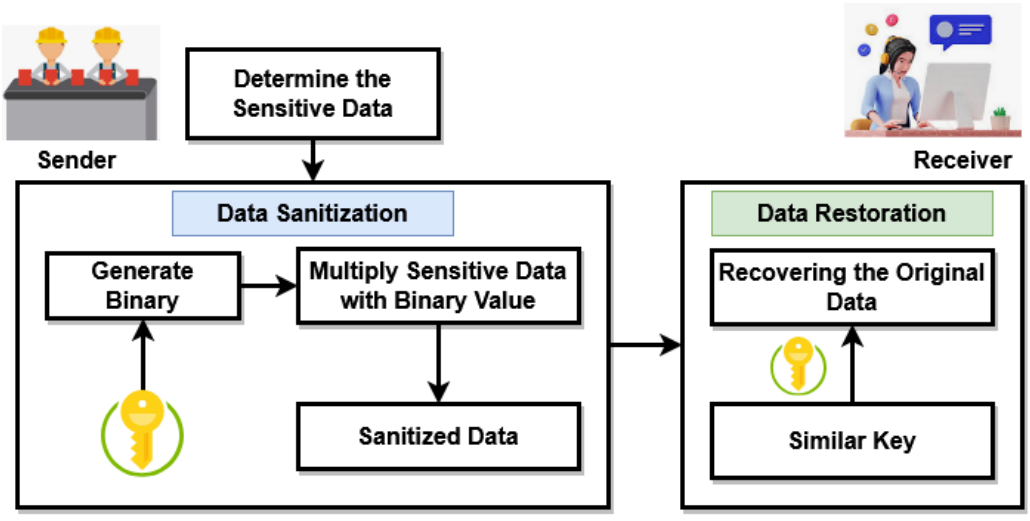

Figure 4. Privacy preservation model.

Moreover, the proposed privacy preservation includes the following operations:

1. Optimal key generation;
2. Sanitization;
3. Restoration.

The process of solution transformation is actually included in the key creation. The Khatri–Rao product is used to change the number of keys K throughout the solution transformation. Initially, the key K can be reconstructed as K_1 with the dimension of $\left[\sqrt{X''_G} \times G_{mx}\right]$, where G_{mx} denotes the maximum number of transactions, and X''_G is the perfect square of the transactions. Here, the matrices K_1 and K_2 are obtained with the use of the Khatri–Rao product. Based on this, the key generation process is carried out, and the metric that is identical to G_{mx} is created. Then, the dimensions are pruned with respect to the length of G_{mx}, and the rule of hiding is applied to get the sanitized data. During the data sanitization process, both the transaction and pruned key matrix are binarized. This data hiding process uses the resulting pruned key matrix to perform the XOR operation, with the binarized data having the same matrix length as that specified in the following equation:

$$G' = \left(K_2 \bigoplus G\right) + 1 \tag{1}$$

Here, the sanitized data G' is obtained with the sanitization key matrix K_2, and the pruned key matrix and transactions are binarized to perform the XOR operation. During the restoration process, the original manufacturer data is obtained from the sanitized data with the same key. In the binarization procedure, the step input is subtracted from the binarized G Following that, the binarized G and the key matrix are subjected to the XOR operation to obtain the restored information, as represented in below:

$$\hat{G} = \left(G' - 1\right) \bigoplus K_2 \tag{2}$$

In order to achieve better data preservation, the objectives, such as the reduction of hiding failure W_1, the degree of modification W_2, the data preservation W_3, and the false rule generation W_4 are minimized, which is mathematically represented below:

$$Objective = minimum(W) = \max(W_1, W_2, W_3, W_4)$$

$$W_1 = \frac{w_1}{\max(w_1)\forall itr} \tag{3}$$

$$W_2 = \frac{w_2}{\max(w_2)\forall itr} \tag{4}$$

$$W_3 = \frac{w_3}{\max(w_3)\forall itr} \tag{5}$$

$$W_4 = \frac{w_4}{\max(w_4)\forall itr} \tag{6}$$

In order to successfully accomplish these objectives, the new optimization technique is used in this work. The suggested PCGS algorithm encodes the keys used in the sanitization procedure. The number of keys is in the range of the key and is optimized using the proposed optimization model, yielding the optimal key, and its length is indicated as $\sqrt{X''_G}$.

3.3. Perceptive Craving Game Search (PCGS) Optimization

In the existing works, several optimization techniques are used to solve complex engineering problems. Due to the increased convergence rate and efficiency, the proposed work uses the PCGS- [51] based optimization algorithm for optimal key generation. This is a meta-heuristics algorithm inspired by the cooperative behavior and hunger-driven actions of animals, given that the PCGS was created using animal behavior in relation to hunger. To construct an adaptable weight, the concept of hunger is used. For effective searching, the authors applied the consequences of hunger to each phase of the search process. The list of symbols used in this PCGS optimization algorithm is presented in Table 2 with its appropriate descriptions. Furthermore, it is divided into two stages:

(1) Acquiring food;
(2) Hunger role.

Table 2. List of symbols and descriptions.

Variables	Descriptions
$P(m)$	Position of all individual
$P^b(m)$	Position of best individual
ω_t' and ω_t''	Weight value
q_1 and q_2	Random numbers [0 to 1]
$r_d(1)$	Normal distributed random number
m	Current iteration
c	Control variable
V	Variation control for all positions
F	Cost function
C^F	Best cost function
j	Population
hyp	Hyperbolic function
$\bar{E}$	Expression
Itr_{max}	Maximum iteration
H	Starvation of each population
K	Population size
H_s	Sum of starving feelings of all populations
New^s	New starvation
$Z(j)$	Cost function value
Low_{bnd}	Lower bound
Up_{bnd}	Upper bound

Individuals' mutual interaction and hunting behavior are described in the first stage, as shown below:

$$P(m+1) = \begin{cases} P(m) * (1 + r_d(1)) & q_1 < c \\ \omega_t' * P^b(m) + \bar{D} * \omega_t'' * \left| P^b(m) - P(m) \right| & q_1 > c, \quad q_2 < V \\ \omega_t' * P^b(m) - \bar{D} * \omega_t'' * \left| P^b(m) - P(m) \right| & q_1 > c, \quad q_2 < V \end{cases} \tag{7}$$

Then, the variation control for all positions is computed based on the following model:

$$V = hyp\left(F(j) - C^F\right) \tag{8}$$

where $C(.)$ Indicates the cost function of population $j \in 1, 2, \ldots, r$, and the hyperbolic function is estimated by using the following model:

$$hyp(x) = \frac{2}{exp^x + exp^{-x}} \tag{9}$$

$$\bar{E} = 2 * b * r_d - b \tag{10}$$

$$b = 2 * \left(1 - \frac{m}{Itr_{max}}\right) \tag{11}$$

The weight values are also computed based on the following models:

$$\omega_t' = \begin{cases} H(j) * \frac{K}{H_s} * q_4 & q_3 < 1 \\ 1 & q_3 \geq 1 \end{cases} \tag{12}$$

$$\omega_t'' = 1 - exp^{(-|H(j) - H_s|) * q_5 * 2} \tag{13}$$

Moreover, the starvation of the population is also estimated according to the following model:

$$H(j) = \begin{cases} 0, & Z(j) == C^C \\ H(j) + New^s & else \end{cases} \tag{14}$$

Based on the actual starvation, the new starvation is estimated as shown below:

$$New^s = Low_{bnd} * (1 - Up_{bnd}) + r_d \tag{15}$$

Finally, the best optimal function is identified and used to optimally generate the key for data sanitization. The working model of the PCGS optimization algorithm is shown in Figure 5.

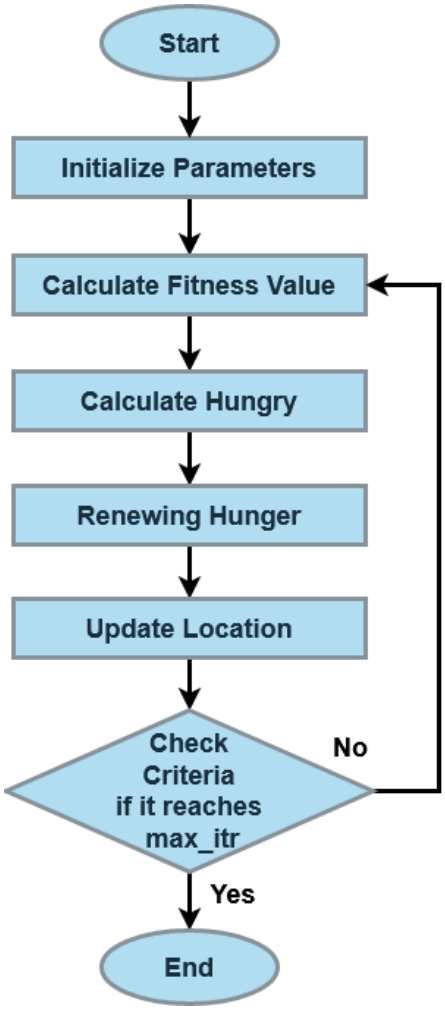

Figure 5. Flow of PCGS.

4. Results and Discussion

This section presents the results and discussion of the existing and proposed optimization-based blockchain methodology used for supply chain management. Blockchains are a cutting-edge technology that, from the standpoint of insight, have the potential to revolutionize current business practices. Blockchain technology is revolutionizing product safety in this context, taking into account its contribution to the real world, due to advancements in accountability. As a result, product provenance will improve life quality and lower the cost of application systems. Blockchain applications have already had an impact on social transformation, environmental sustainability, and even the preservation of the environment. For performance assessment, the dataset named Dataco_Smart_Supply_Chain, obtained from Kaggle [52], has been used in this work. Here, various optimization techniques, such as particle swarm optimization (PSO) [53], grey wolf optimization (GWO) [54], firefly optimization (FFO) [55], artificial bee colony (ABC) [56], and jellyfish optimization (JFO) [57], are considered for comparative analysis. Moreover, various measures, such as efficiency, key sensitivity, correlation coefficient, etc., are used for validating the results.

Here, the optimization efficacy of the proposed PCGS algorithm is validated according to the parameters of the best score, fitness plot, and searching history. As shown in Figure 6, the best score obtained by using the proposed PCGS mechanism concerning different iterations is validated. Solving problems with many variables and restrictions is typically a time-consuming and difficult task. Moreover, many local optimum solutions do not ensure the greatest outcome when utilizing conventional numerical techniques. Therefore, the PCGS technique is utilized in the proposed work, which obtains the best optimal solution for generating a key to perform data sanitization. The observed results indicate that the PCGS reaches the best score with a minimal number of iterations. Similarly, the fitness plot and search history of this optimization technique are represented in Figures 7 and 8, respectively. Then, the convergence analysis is depicted in Figure 9. The objective score that represents the average of all particles during each iteration is known as average fitness. It demonstrates how the proposed PCGS algorithm enhances the optimum accuracy during simulation runs. Moreover, the PCGS algorithm explores the whole search space and does not get caught in local optima. The distribution of sample points is centered on the actual optimal solution, ensuring the viability of its application. Thus, the proposed PCGS is capable of both exploration and exploitation. Overall, this analysis indicates that the proposed PCGS provides better performance by effectively identifying the best fitness, with minimal iterations in the search space.

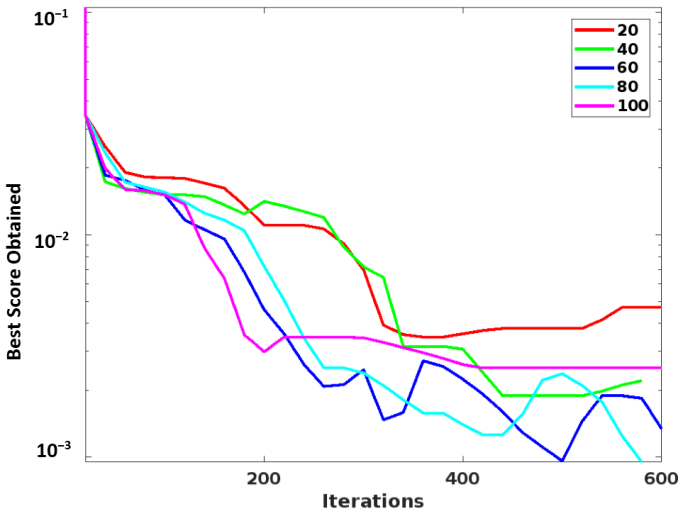

Figure 6. Best score analysis.

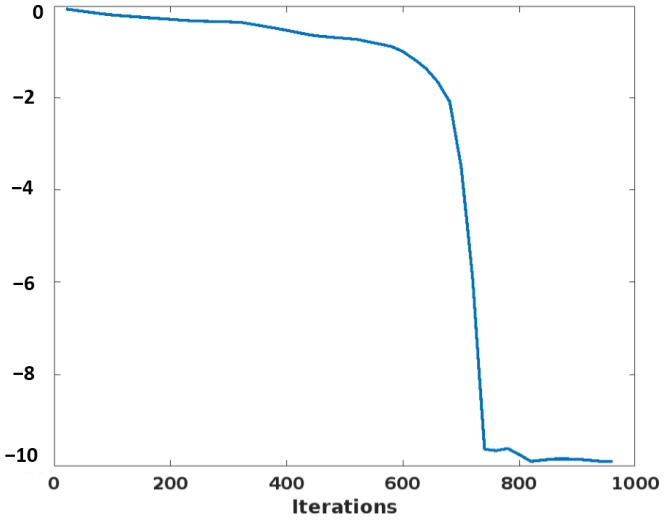

Figure 7. Fitness plot of the proposed PCGS optimization technique.

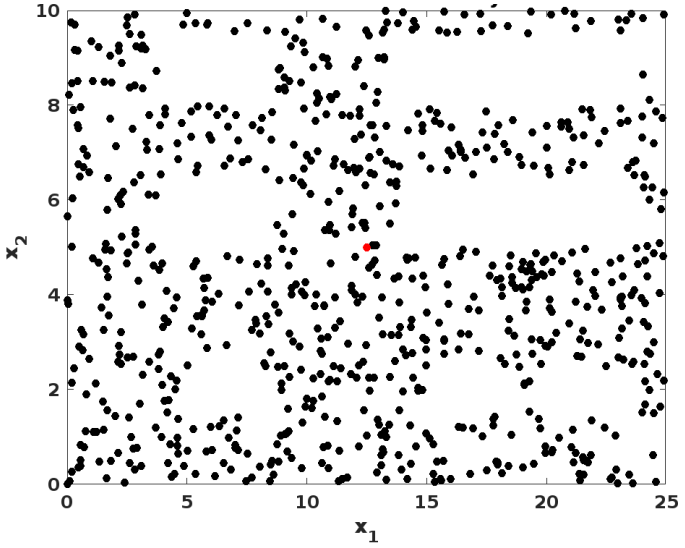

Figure 8. Searching history of the PCGS.

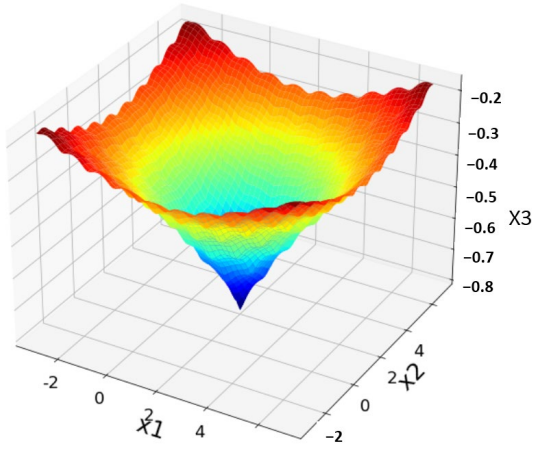

Figure 9. Convergence analysis.

Figure 10 compares the optimization cost of the baseline and proposed optimization algorithms with respect to a varying number of iterations. In order to validate the

performance of the proposed PCGS optimization technique used for key generation, the convergence rate, cost function, and key sensitivity have been estimated. Moreover, the effectiveness of the blockchain integrated privacy preservation model used in the SCM is validated and compared using the utility and privacy parameters. Overall, the estimated outcomes state that the PCGS model provides an improved and reliable outcome, when compared to that of the other techniques. The cost function is a performance metric that expresses the viability of the proposed work. The PCGS outperforms the other baseline models with a lower cost function, as shown by the results. Due to its improved exploration and exploitation capability, the results of the proposed PCGS are effectively improved in this work. Moreover, the key sensitivity is validated and compared to key variation (%), as shown in Figure 11. By changing the percentage level of the key from 10% to 50%, the ideal key sensitivity is assessed. The obtained results indicated that the PCGS effectively minimized the key sensitivity for all variations. In addition to that, the correlation coefficient is also validated and compared to the variation of the key (%), as shown in Table 3 and Figure 12. Moreover, there should be little correlation between the sanitized data and the key, with deviation. When compared to other conventional models, the proposed scheme achieves the lowest correlation, as illustrated by the graphic in Figure 12. Moreover, the correlation obtained by the proposed PCGS is 0.5%, which is significantly better than that obtained by other approaches.

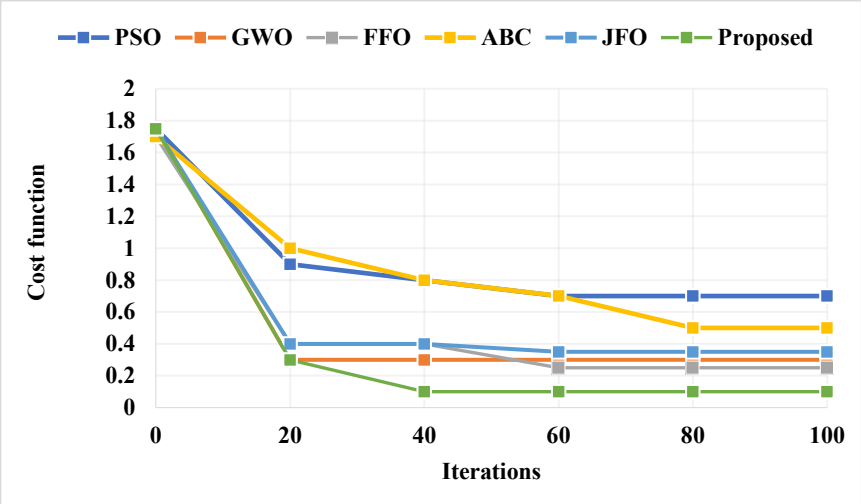

Figure 10. Optimization cost function.

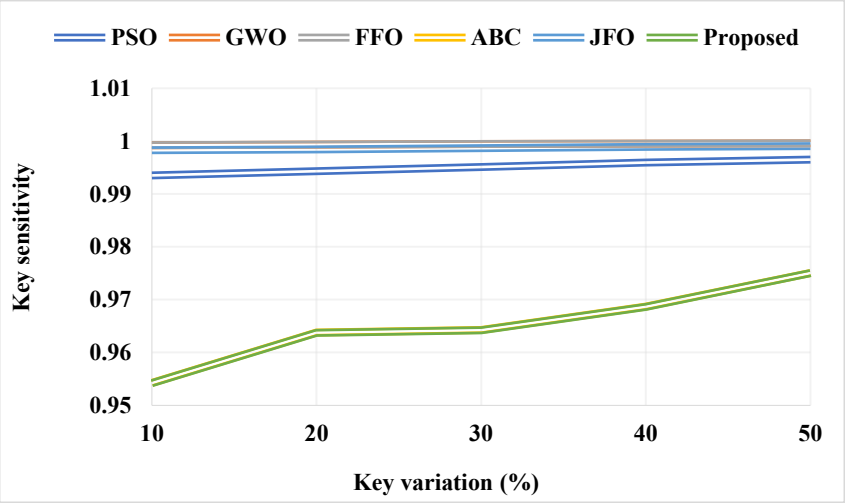

Figure 11. Key sensitivity.

Table 3. Analysis of correlation coefficient.

Variation of Key (%)	PSO	GWO	FFO	ABC	JFO	Proposed
10	0.9	0.9	0.89	0.89	0.85	0.8
30	0.82	0.83	0.84	0.81	0.81	0.75
40	0.9	0.92	0.92	0.91	0.89	0.85
50	0.82	0.8	0.79	0.79	0.75	0.7
70	0.6	0.59	0.59	0.55	0.54	0.5

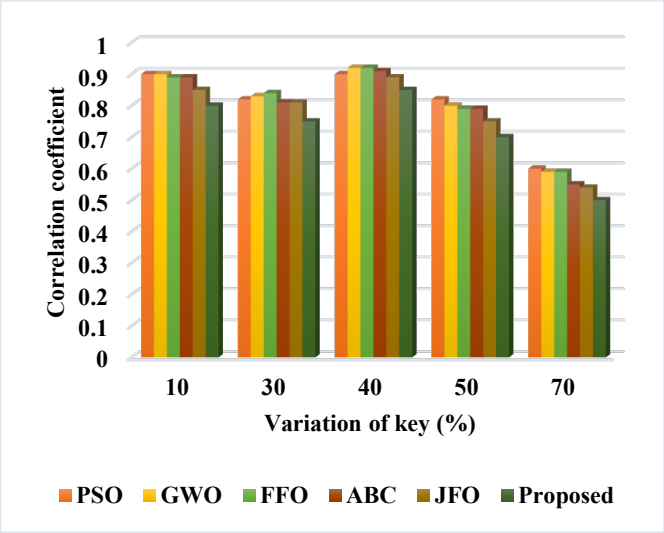

Figure 12. Comparison based on correlation coefficient.

Figure 13 illustrates the findings obtained after comparing the Euclidean distance between the existing and proposed methodologies. When compared to the other works, the proposed study shows the lowest Euclidean distance for the given logistics dataset. It also shows the results of computing the Euclidean distance in terms of harmonic mean. This analysis also indicates that both the Euclidean distance and the harmonic mean have been effectively reduced in the proposed work when compared to the other baseline models. In addition, the Pearson coefficient (PC) and the Spearman coefficient (SC) of the baseline and proposed optimization models is shown in Figure 14. A set of the expected data's arithmetic mean is calculated by dividing the total number of observations by the sum of all the numerical values for each observation. Here, the arithmetic mean is validated in terms of PC and SC. For an effective and secure data transfer, both PC and SC must be low. When compared to the current models, the PC and SC of the proposed work reveal few variances. However, as a whole, it is claimed that the cost function's overall target is lower, and as a result, it achieves an improved level of protected data transfer.

Table 4 and Figure 15 compare the sanitization and restoration efficiency of the existing and proposed optimization models. Typically, the efficiency level of both data sanitization and restoration operations are validated for determining how effectively the privacy preservation model ensures the security of logistics data. Based on the outcomes, it is concluded that the proposed PCGS provides an increased sanitization and restoration efficiency when compared to the standard optimization models.

Furthermore, the sanitization efficiency of the existing and proposed optimization algorithms are validated and compared to the different counts of sanitized data, as shown in Table 5 and Figure 16. Similarly, the restoration efficiency concerning the count of data is compared, as shown in Table 6 and Figure 17. Both analyses indicate that the proposed PCGS algorithm overwhelms the standard optimization models with increased data sanitization and restoration efficiency. Therefore, the overall privacy preservation

level of the proposed blockchain-based supply chain management framework is effectively improved, when contrasted with that of the other techniques.

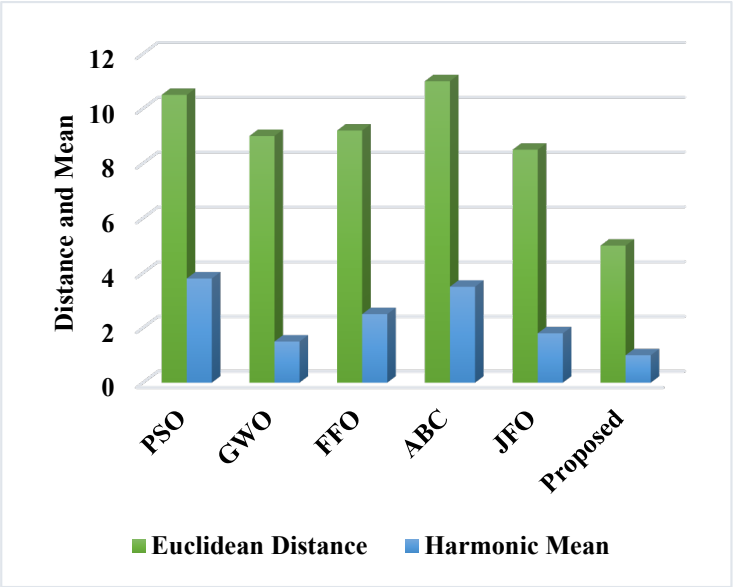

Figure 13. Euclidean distance and harmonic mean.

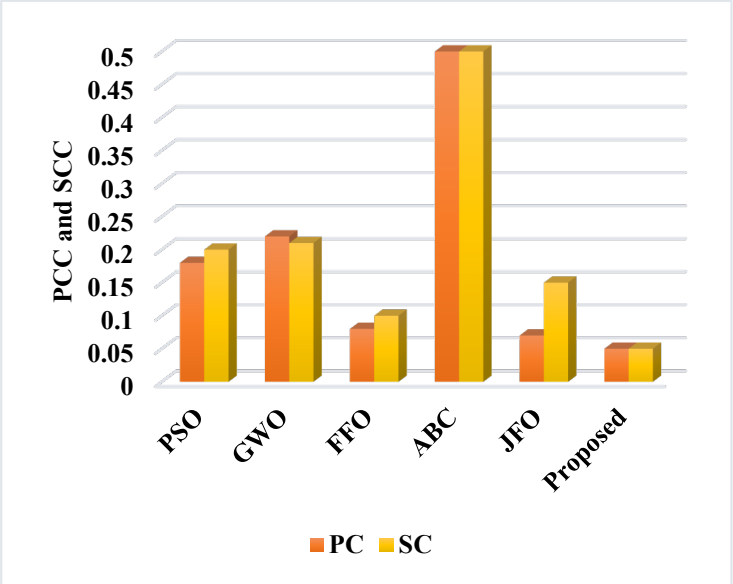

Figure 14. Comparative analysis based on PC and SC.

Table 4. Efficiency analysis.

Methods	Efficiency of Sanitization (%)	Efficiency of Restoration (%)
PSO	66	91
GWO	47	95
FFO	58	96
ABC	69	94
JFO	86	97
Proposed	98	98.5

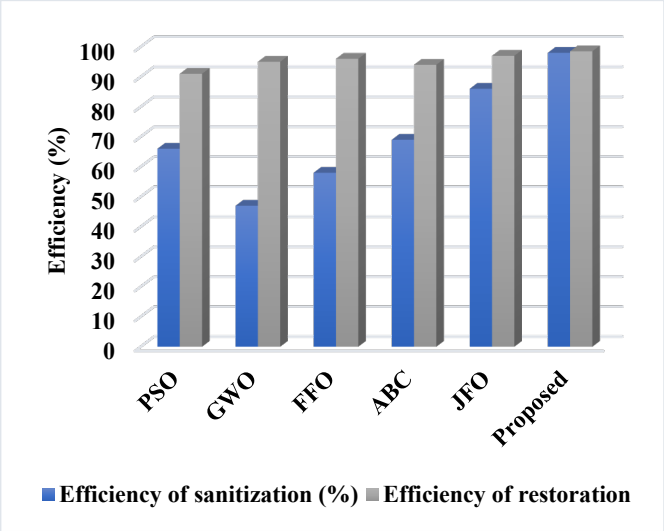

Figure 15. Sanitization and restoration efficiency analysis.

Table 5. Sanitization efficiency analysis.

Sanitized Data	PSO	GWO	FFO	ABC	JFO	Proposed
1	81	78	90	91	95	99
2	80	77	87	88	92	98.9
3	78	73	85	85	90	98.5
4	73	69	80	80	84	97.4
5	70	65	78	79	80	96.9

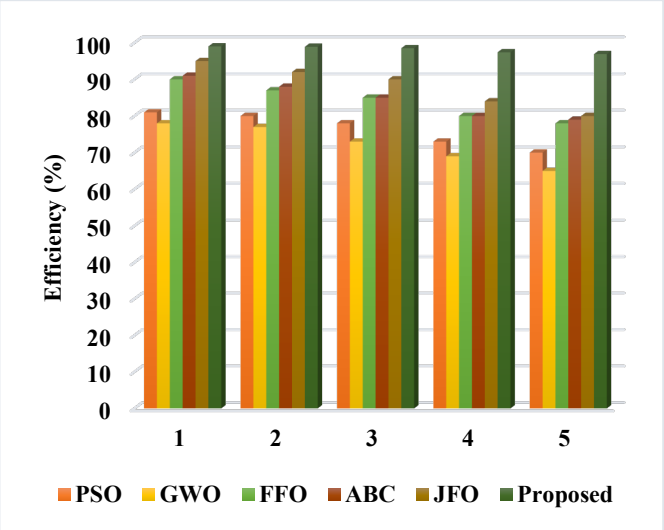

Figure 16. Comparison based on sanitization efficiency.

Figures 18 and 19 validate and compare the cost function and privacy of the existing [58] and proposed blockchain-based privacy preservation models. Consequently, the statistical analysis is also carried out in this work for validating the results of the optimization integrated blockchain models, as shown in Tables 7 and 8. Moreover, the improved privacy and utility values ensure the better performance of the security framework. According to the results, it is obvious that the proposed PCGS-based privacy preservation model provides effective results when compared to those of the other algorithms.

Table 6. Restoration efficiency analysis.

Sanitized Data	PSO	GWO	FFO	ABC	JFO	Proposed
1	88	91	91	92	96	99.5
2	85	89	90	90	94.5	99.2
3	82	85	88	89	94	99
4	80	82	86	85	92	98.9
5	79	81	84	83	90	98.5

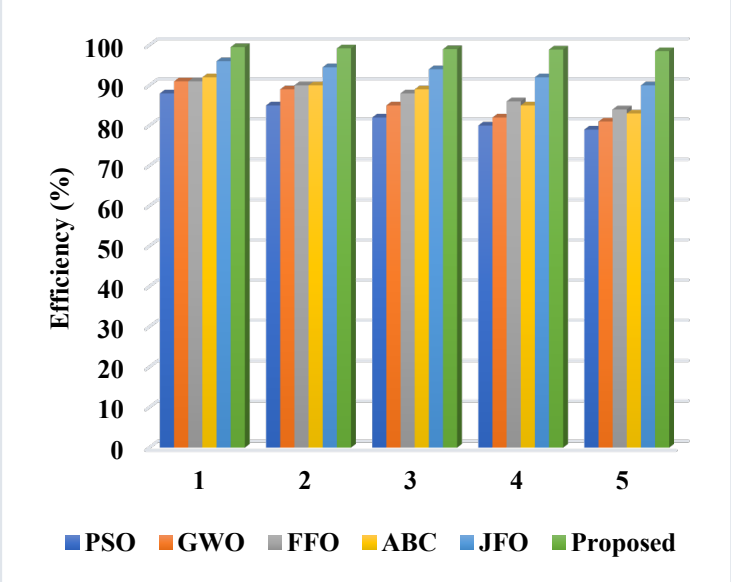

Figure 17. Comparison based on restoration efficiency.

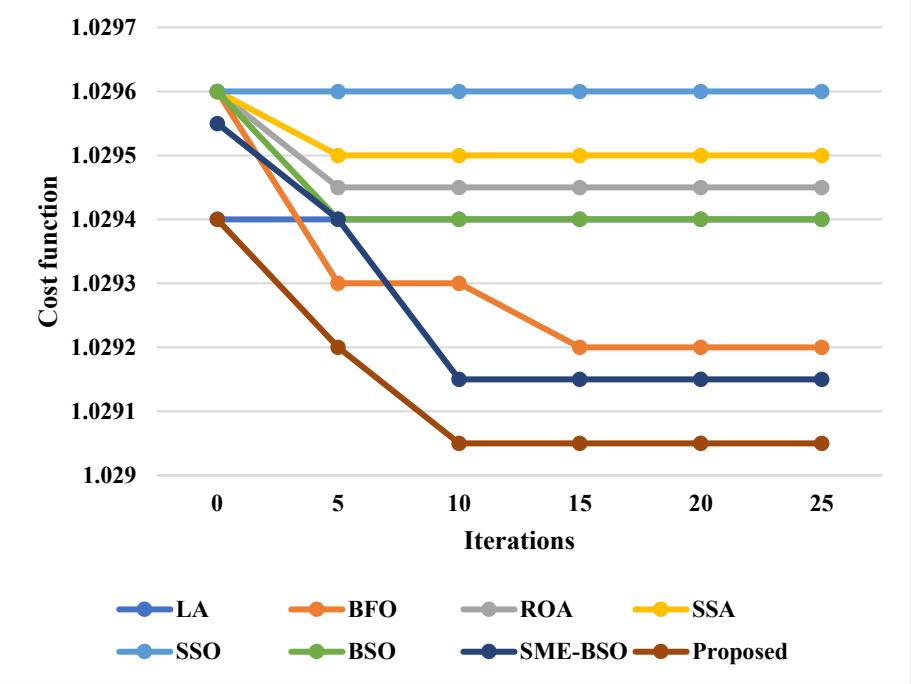

Figure 18. Comparative analysis based on cost function.

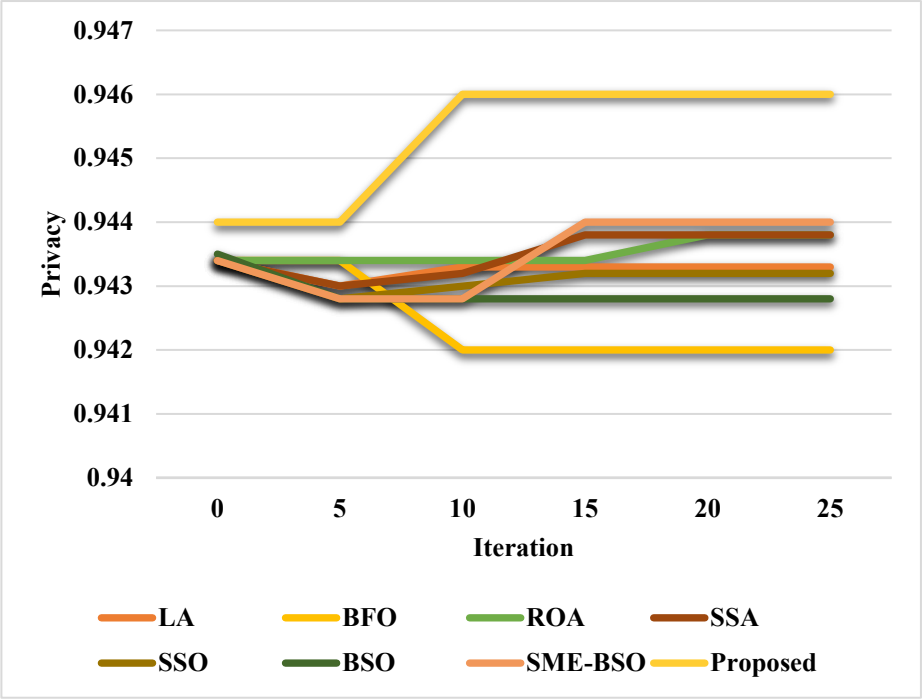

Figure 19. Comparative analysis based on privacy.

Table 7. Statistical analysis based on utility.

Measures	LA	BFO	ROA	SSA	SSO	BSO	SME-BSO	Proposed
Mean	0.99924	0.99974	0.99917	0.99978	0.99909	0.99959	0.99991	0.99992
Best	0.99966	0.99989	0.99923	0.99985	0.99911	0.99967	0.99998	0.99999
Median	0.99905	0.99971	0.99922	0.99985	0.9991	0.99967	0.99998	0.99998
Worst	0.99905	0.99905	0.99905	0.99905	0.99905	0.99905	0.99905	0.99905

Table 8. Statistical analysis based on privacy.

Measures	LA	BFO	ROA	SSA	SSO	BSO	SME-BSO	Proposed
Worst	0.94282	0.94341	0.94341	0.94282	0.94341	0.94282	0.94282	0.94281
Best	0.94344	0.94388	0.94384	0.94382	0.94344	0.94344	0.94411	0.9468
Mean	0.94344	0.94375	0.94359	0.94351	0.94342	0.94289	0.94369	0.9462
Median	0.94327	0.94388	0.94344	0.94382	0.94341	0.94282	0.94411	0.9468

5. Conclusions

This paper presents a new blockchain-based privacy preservation framework for ensuring the safety of the supply chain management system. Here, the PCGS optimization technique is used to develop an ideal key, which is then used to sanitize the original logistics data that was collected from the manufacturer. More specifically, when uploading all of the cleaned data over a single blockchain, there is a risk of unauthorized access and data swarm that slows down the system. Additionally, the sanitized data from the sender is sent here via several sub-chains to the authorized parties. The original data is recovered from the sanitized data at the other end. Both the data sanitization and restoration procedures rely heavily on key generation, which must be properly selected. With the aid of the PCGS optimization algorithm, the key utilized for data sanitization in this case is optimally created. By using the right key, the provider can access the original data and recover the sensitive information. For analysis, the original SCM data, such as

"SCMS_Delivery_History_Dataset" and "Dataset of Supply Chains used by the company DataCo Global" have been used to validate and compare the results of the proposed blockchain-enabled PCGS privacy preservation model. Provisioning, manufacturing, sales, and corporate distribution are areas with significant registered operations that can be used with machine learning algorithms and software. The performance and results of the proposed privacy preservation framework are validated by using different parameters, including key sensitivity, sanitization efficiency, restoration efficiency, correlation coefficient, etc. From the observed results, it is concluded that the PCGS-based privacy preservation model provides improved outcomes over those of the baseline models, with improved efficacy. Due to privacy and security issues, supply chain experts may not be willing to disclose crucial information, since they see information confidentiality as key to their competitive advantage. Through participant anonymity, the blockchain upholds the privacy of the information that is transparently stored. Even if the participants' identities are unknown, shared transactional information may improve supply chain performance. The privacy preservation model is a crucial part of the business information system and can give organizations a competitive edge by enabling them to maintain a secured and legal supply chain. However, the proposed PCGS-based privacy preservation model has the following major challenges: it restricts the capacity to precisely gather, maintain, and query data for product identification and tracking. Moreover, due to the necessity of maintaining the complete history of all blocks and transactions across all blockchain network participants, the blockchain has a limited storage capacity. Furthermore, the efficiency and traceability of supply chains systems is constrained by the requirement to secure the confidentiality, privacy, and dependability of tracking data. High resilience is achieved by eliminating central processing and having every party maintain a local copy of the entire set of traceable data. Although reporting can be conducted against local instances of the data, since data connection across distributed data stores is a fundamental component of blockchain design, the availability of the data is constrained by the rate at which it spreads. In other words, the ability to report the current condition is constrained by the delay.

In the future, the present work can be enhanced by implementing this system in a real-time application.

Author Contributions: Conceptualization, B.A. and M.A.O.; methodology, B.A. and M.A.O.; software, B.A. and M.A.O.; validation, B.A. and M.A.O.; formal analysis, B.A. and M.A.O.; investigation, B.A. and M.A.O.; writing B.A. and M.A.O.; review and editing, B.A. and M.A.O.; visualization, B.A. and M.A.O.; supervision, M.A.O.; project administration, M.A.O. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The data presented in this study are available on request from the corresponding author.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Abdallah, S.; Nizamuddin, N. Blockchain-based solution for Pharma Supply Chain Industry. *Comput. Ind. Eng.* **2023**, *177*, 108997. [CrossRef]
2. Agarwal, U.; Rishiwal, V.; Tanwar, S.; Chaudhary, R.; Sharma, G.; Bokoro, P.N.; Sharma, R. Blockchain Technology for Secure Supply Chain Management: A Comprehensive Review. *IEEE Access* **2022**, *10*, 85493–85517. [CrossRef]
3. Akuns, U.; Okafor, S. Big data analytics: Virtuosity in Lean Six Sigma for quality assurance in supply chain management. *Interdiscip. J. Econ. Bus. Law* **2022**, *11*, 44–72.
4. Alhazami, L.; Rachmawati, A. Supply Chain Management Information System Analysis In Services Private Banks. *Int. J. Manag. Bus. Soc. Sci.* **2022**, *1*, 2.

5. Ali, S.; Anwar, W.; Salem, B.J.; Al Dhuhlia, M. Tracing Pharmaceutical Products Utilizing Blockchain Technologies. *Int. J. Comput. Digit. Syst.* **2022**, *12*, 1174–1181. [CrossRef]
6. Alkahtani, M. Supply Chain Management Optimization and Prediction Model Based on Projected Stochastic Gradient. *Sustainability* **2022**, *14*, 3486. [CrossRef]
7. Baryannis, G.; Validi, S.; Dani, S.; Antoniou, G. Supply chain risk management and artificial intelligence: State of the art and future research directions. *Int. J. Prod. Res.* **2019**, *57*, 2179–2202. [CrossRef]
8. Bhatia, S.; Albarrak, A.S. A Blockchain-Driven Food Supply Chain Management Using QR Code and XAI-Faster RCNN Architecture. *Sustainability* **2023**, *15*, 2579. [CrossRef]
9. Chang, S.E.; Chen, Y. When Blockchain Meets Supply Chain: A Systematic Literature Review on Current Development and Potential Applications. *IEEE Access* **2020**, *8*, 62478–62494. [CrossRef]
10. Chen, S.; Shen, Z.; Zhang, L.; Yan, Z.; Li, C.; Wu, J. A trusted energy trading framework by marrying blockchain and optimization. *Adv. Appl. Energy* **2021**, *2*, 100029. [CrossRef]
11. Chennam, K.K.; Aluvalu, R.; Shitharth, S. An Authentication Model with High Security for Cloud Database. In *Architectural Wireless Networks Solutions and Security Issues*; Das, S.K., Samanta, S., Dey, N., Patel, B.S., Hassanien, A.E., Eds.; Springer: Singapore, 2021; pp. 13–25.
12. Chou, J.-S.; Molla, A. Recent advances in use of bio-inspired jellyfish search algorithm for solving optimization problems. *Sci. Rep.* **2022**, *12*, 19157. [CrossRef] [PubMed]
13. Deliktaş, D.; Karagoz, S.; Simić, V.; Aydin, N. A stochastic Fermatean fuzzy-based multi-choice conic goal programming approach for sustainable supply chain management in end-of-life buildings. *J. Clean. Prod.* **2023**, *382*, 135305. [CrossRef]
14. Dokeroglu, T.; Sevinc, E.; Cosar, A. Artificial bee colony optimization for the quadratic assignment problem. *Appl. Soft Comput.* **2019**, *76*, 595–606. [CrossRef]
15. Dolatabad, M.J.; Azhdarifard, M.; Dwijendra, N.K.A.; Al-Sudani, A.Q.A.S. Evaluating Agile Practices in Green Supply Chain Management Using a Fuzzy Multicriteria Approach. *Discret. Dyn. Nat. Soc.* **2022**, *2022*, 4290848. [CrossRef]
16. Fan, Y.; Stevenson, M. A review of supply chain risk management: Definition, theory, and research agenda. *Int. J. Phys. Distrib. Logist. Manag.* **2018**, *48*, 205–230. [CrossRef]
17. Gupta, P.; Hudnurkar, M.; Ambekar, S. Effectiveness of blockchain to solve the interoperability challenges in healthcare. *Cardiometry* **2021**, *20*, 80–88. [CrossRef]
18. Gurtu, A.; Johny, J. Supply Chain Risk Management: Literature Review. *Risks* **2021**, *9*, 16. [CrossRef]
19. Heidari, S.S.; Khanbabaei, M.; Sabzehparvar, M. A model for supply chain risk management in the automotive industry using fuzzy analytic hierarchy process and fuzzy TOPSIS. *Benchmarking Int. J.* **2018**, *25*, 3831–3857. [CrossRef]
20. Houssein, E.H.; Gad, A.G.; Hussain, K.; Suganthan, P.N. Major Advances in Particle Swarm Optimization: Theory, Analysis, and Application. *Swarm Evol. Comput.* **2021**, *63*, 100868. [CrossRef]
21. Hu, H.; Xu, J.; Liu, M.; Lim, M.K. Vaccine supply chain management: An intelligent system utilizing blockchain, IoT and machine learning. *J. Bus. Res.* **2023**, *156*. [CrossRef] [PubMed]
22. Jamil, F.; Hang, L.; Kim, K.; Kim, D. A Novel Medical Blockchain Model for Drug Supply Chain Integrity Management in a Smart Hospital. *Electronics* **2019**, *8*, 505. [CrossRef]
23. Kalyani, D.; Pradeep, S.; Srivani, P. Secured information sharing in SCM: Parametric Analysis on Improved Beetle Swarm Optimization. *Procedia Comput. Sci.* **2022**, *215*, 897–908. [CrossRef]
24. Kara, M.E.; Fırat, S.O.; Ghadge, A. A data mining-based framework for supply chain risk management. *Comput. Ind. Eng.* **2020**, *139*, 105570. [CrossRef]
25. Kashem, M.A.; Shamsuddoha, M.; Nasir, T.; Chowdhury, A.A. Supply Chain Disruption versus Optimization: A Review on Artificial Intelligence and Blockchain. *Knowledge* **2023**, *3*, 80–96. [CrossRef]
26. Khor, J.H.; Sidorov, M.; Zulqarnain, S.A.B. Scalable Lightweight Protocol for Interoperable Public Blockchain-Based Supply Chain Ownership Management. *Sensors* **2023**, *23*, 3433. [CrossRef] [PubMed]
27. Kumar, A.; Bhushan, B.; Shristi, S.; Kalita, S.; Chaganti, R.; Obaid, A.J. Blockchain Embedded Security and Privacy Preserving. In *Healthcare Systems Blockchain Technology Solutions for the Security of Iot-Based Healthcare Systems*; Elsevier: Amsterdam, The Netherlands, 2023; pp. 241–261.
28. Kumar, M.; Aggarwal, J.; Rani, A.; Stephan, T.; Shankar, A.; Mirjalili, S. Secure video communication using firefly optimization and visual cryptography. *Artif. Intell. Rev.* **2021**, *55*, 2997–3017. [CrossRef]
29. Lin, X. Network Security Technology of Supply Chain Management Based on Internet of Things and Big Data. *Comput. Intell. Neurosci.* **2022**, *2022*, 7753086. [CrossRef]
30. Liu, K.-S.; Lin, M.-H. Performance Assessment on the Application of Artificial Intelligence to Sustainable Supply Chain Management in the Construction Material Industry. *Sustainability* **2021**, *13*, 12767. [CrossRef]
31. Lohmer, J.; da Silva, E.R.; Lasch, R. Blockchain Technology in Operations & Supply Chain Management: A Content Analysis. *Sustainability* **2022**, *14*, 6192. [CrossRef]
32. Lotfi, R.; Safavi, S.; Gharehbaghi, A.; Zare, S.G.; Hazrati, R.; Weber, G.-W. Viable Supply Chain Network Design by considering Blockchain Technology and Cryptocurrency. *Math. Probl. Eng.* **2021**, *2021*, 7347389. [CrossRef]
33. Malhotra, P.; Singh, Y.; Anand, P.; Bangotra, D.; Singh, P.; Hong, W.-C. Internet of Things: Evolution, Concerns and Security Challenges. *Sensors* **2021**, *21*, 1809. [CrossRef] [PubMed]

34. Nadimi-Shahraki, M.H.; Taghian, S.; Mirjalili, S. An improved grey wolf optimizer for solving engineering problems. *Expert Syst. Appl.* **2021**, *166*, 113917. [CrossRef]
35. Obaidat, M.A.; Brown, J. Perspectives of Blockchain. In *Cybersecurity: Applications and Future Developments Research Anthology on Convergence of Blockchain, Internet of Things, and Security*; IGI Global: Hershey, PA, USA, 2023; pp. 818–840.
36. Obaidat, M.A.; Obeidat, S.; Holst, J.; Al Hayajneh, A.; Brown, J. A Comprehensive and Systematic Survey on the Internet of Things: Security and Privacy Challenges, Security Frameworks, Enabling Technologies, Threats, Vulnerabilities and Countermeasures. *Computers* **2020**, *9*, 44. [CrossRef]
37. Oliveira, J.; Jin, M.; Lima, R.D.S.; Kobza, J.; Montevechi, J. The role of simulation and optimization methods in supply chain risk management: Performance and review standpoints. *Simul. Model. Pract. Theory* **2019**, *92*, 17–44. [CrossRef]
38. Pournader, M.; Kach, A.; Talluri, S. A Review of the Existing and Emerging Topics in the Supply Chain Risk Management Literature. *Decis. Sci.* **2020**, *51*, 867–919. [CrossRef] [PubMed]
39. Putri, A.N.; Hariadi, M.; Wibawa, A.D. Smart Agriculture Using Supply Chain Management Based on Hyperledger Blockchain. *IOP Conf. Ser. Earth Environ. Sci.* **2020**, *466*, 012007. [CrossRef]
40. Santhi, A.R.; Muthuswamy, P. Influence of Blockchain Technology in Manufacturing Supply Chain and Logistics. *Logistics* **2022**, *6*, 15. [CrossRef]
41. Ravi, D.; Ramachandran, S.; Vignesh, R.; Falmari, V.R.; Brindha, M. Privacy preserving transparent supply chain management through Hyperledger Fabric. *Blockchain Res. Appl.* **2022**, *3*, 100072. [CrossRef]
42. Rostamzadeh, R.; Ghorabaee, M.K.; Govindan, K.; Esmaeili, A.; Nobar, H.B.K. Evaluation of sustainable supply chain risk management using an integrated fuzzy TOPSIS- CRITIC approach. *J. Clean. Prod.* **2018**, *175*, 651–669. [CrossRef]
43. Sachdev, D. Enabling data democracy in supply chain using blockchain and iot. *J. Manag.* **2019**, *6*, 66–83. [CrossRef]
44. Salamai, A.; Hussain, O.K.; Saberi, M.; Chang, E.; Hussain, F.K. Highlighting the Importance of Considering the Impacts of Both External and Internal Risk Factors on Operational Parameters to Improve Supply Chain Risk Management. *IEEE Access* **2019**, *7*, 49297–49315. [CrossRef]
45. Selvarajan, S.; Shaik, M.; Ameerjohn, S.; Kannan, S. Mining of intrusion attack in SCADA network using clustering and genetically seeded flora-based optimal classification algorithm. *IET Inf. Secur.* **2020**, *14*, 1–11. [CrossRef]
46. Sharma, P.; Namasudra, S.; Crespo, R.G.; Parra-Fuente, J.; Trivedi, M.C. EHDHE: Enhancing Security of Healthcare Documents in IoT-enabled Digital Healthcare Ecosystems using Blockchain. *Inf. Sci.* **2023**, *629*, 703–718. [CrossRef]
47. Shekarian, E.; Ijadi, B.; Zare, A.; Majava, J. Sustainable Supply Chain Management: A Comprehensive Systematic Review of Industrial Practices. *Sustainability* **2022**, *14*, 7892. [CrossRef]
48. Sodhro, A.H.; Pirbhulal, S.; Muzammal, M.; Zongwei, L. Towards Blockchain-Enabled Security Technique for Industrial Internet of Things Based Decentralized Applications. *J. Grid Comput.* **2020**, *18*, 615–628. [CrossRef]
49. Sugara, A.A.; Azis, A.M. Electronic supply chain management application analysis in retail industry. *Int. J. Bus. Technol. Manag.* **2020**, *2*, 45–51.
50. Tanwar, S.; Bhatia, Q.; Patel, P.; Kumari, A.; Singh, P.K.; Hong, W.-C. Machine Learning Adoption in Blockchain-Based Smart Applications: The Challenges, and a Way Forward. *IEEE Access* **2020**, *8*, 474–488. [CrossRef]
51. Tijan, E.; Aksentijević, S.; Ivanić, K.; Jardas, M. Blockchain Technology Implementation in Logistics. *Sustainability* **2019**, *11*, 1185. [CrossRef]
52. Tiwari, S. DataCo Smart Supply Chain for Big Data Analysis. Available online: https://www.kaggle.com/datasets/shashwatwork/dataco-smart-supply-chain-for-big-data-analysis (accessed on 12 April 2020).
53. Wenhua, Z.; Qamar, F.; Abdali, T.-A.N.; Hassan, R.; Jafri, S.T.A.; Nguyen, Q.N. Blockchain Technology: Security Issues, Healthcare Applications, Challenges and Future Trends. *Electronics* **2023**, *12*, 546. [CrossRef]
54. Wong, S.; Yeung, J.-K.-W.; Lau, Y.-Y.; So, J. Technical Sustainability of Cloud-Based Blockchain Integrated with Machine Learning for Supply Chain Management. *Sustainability* **2021**, *13*, 8270. [CrossRef]
55. Yang, Y.; Chen, H.; Heidari, A.A.; Gandomi, A.H. Hunger games search: Visions, conception, implementation, deep analysis, perspectives, and towards performance shifts. *Expert Syst. Appl.* **2021**, *177*, 114864. [CrossRef]
56. Yue, Y.; Fu, X. Research on Medical Equipment Supply Chain Management Method Based on Blockchain Technology. In Proceedings of the International Conference on Service Science (ICSS), Xining, China, 24–26 August 2020; pp. 143–148. [CrossRef]
57. Zekhnini, K.; Cherrafi, A.; Bouhaddou, I.; Benghabrit, Y.; Garza-Reyes, J.A. Supply chain management 4.0: A literature review and research framework. *Benchmarking Int. J.* **2021**, *28*, 465–501. [CrossRef]
58. Zkik, K.; Sebbar, A.; Nejjari, N.; Lahlou, S.; Fadi, O.; Oudani, M. Secure Model for Records Traceability. In *Airline Supply Chain Based on Blockchain and Machine Learning Digital Transformation and Industry 4.0 for Sustainable Supply Chain Performance*; Springer: Berlin/Heidelberg, Germany, 2023; pp. 141–159.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.