Article

Securing Blockchain-Based Supply Chain Management: Textual Data Encryption and Access Control

Imran Khan 1,†, Qazi Ejaz Ali 1,†, Hassan Jalil Hadi 2,*,†, Naveed Ahmad 3,†, Gauhar Ali 3,†, Yue Cao 2,† and Mohammed Ali Alshara 3,4,†

1 Department of Computer Science, University of Peshawar, Peshawar 24701, Pakistan
2 School of Cyber Science and Engineering, Wuhan University, Wuhan 430072, China; yue.cao@whu.edu.cn
3 College of Computer and Information Sciences, Prince Sultan University, Riyadh 11586, Saudi Arabia; nahmed@psu.edu.sa (N.A.); malshara@psu.edu.sa (M.A.A.)
4 College of Computer Sciences and Information for Educational and Quality Affairs, Al-Imam Muhammad Ibn Saud Islamic University, Riyadh 11432, Saudi Arabia
* Correspondence: hjhwhu@whu.edu.cn
† These authors contributed equally to this work.

Abstract: A supply chain (SC) encompasses a network of businesses, individuals, events, data, and resources orchestrating the movement of goods or services from suppliers to customers. Leveraging a blockchain-based platform, smart contracts play a pivotal role in aligning business logic and tracking progress within supply chain activities. Employing two distinct ledgers, namely Hyperledger and Ethereum, introduces challenges in handling the escalating volume of data and addressing the technical expertise gap related to supply chain management (SCM) tools in blockchain technology. Within the domain of blockchain-based SCM, the growing volume of data activities introduces challenges in the efficient regulation of data flow and the assurance of privacy. To tackle these challenges, a straightforward approach is recommended to manage data growth and thwart unauthorized entries or spam attempts within blockchain ledgers. The proposed technique focuses on validating hashes to ensure blockchain integrity. Emphasizing the authentication of sensitive data on the blockchain to bolster SCM, this approach compels applications to shoulder increased accountability. The suggested technique involves converting all data into textual format, implementing code encryption, and establishing permission-based access control. This strategy aims to address inherent weaknesses in blockchain within SCM. The results demonstrate the efficacy of the proposed technique in providing security and privacy for various types of data within SCM. Overall, the approach enhances the robustness of blockchain-based SCM, offering a comprehensive solution to navigate evolving challenges in data management and privacy assurance.

Keywords: supply chain management; blockchain; security; authentication; Hyperledger Fabric; ethereum blockchain

1. Introduction

A supply chain (SC) encompasses a consortium of firms, individuals, activities, data, and resources involved in the seamless movement of a product or service from the supplier to the client [1,2]. Chang et al. [3] assert that smart contracts play a pivotal role in establishing a connection between business logic and progress monitoring in supply chain operations through a blockchain-based platform. Blockchain, a recently developed distributed information system, is crucial for maintaining the quality of sensitive items during transportation. As elucidated in [4], this is imperative because centralized SCM systems are susceptible to issues such as cheating, fraud, and manipulation. Blockchain technology in supply chain management establishes a transparent and secure system for tracking the flow of items and validating their authenticity. It ensures end-to-end visibility and accountability by facilitating real-time data and information exchange among
stakeholders. The pursuit of reliable management is a common objective for many businesses, with a focus on leveraging suitable technologies [4]. Consequently, companies are directing their efforts toward adopting technologies that can meet the demands of supply chain management. Blockchain is increasingly employed in various supply chain applications, primarily to enhance financial and trust-related aspects efficiently [5]. When using a blockchain for security purposes, two ledgers are employed. Ethereum and Hyperledger are the two blockchain platforms available. Ethereum is a distributed ledger system that is open to the public. Hyperledger is a blockchain network with limited access, which can secure transactions [6]. All transactions on the network are only visible to organizations or individuals that hold a licensing certificate [7]. Working with blockchain-based supply chain management does provide some challenges; similar to managing the increasing amount of data as the volume of data activities is increasing, there is a lack of technical expertise on the supply chain tools employed by blockchain technology.

Managing privacy and data flow in blockchain applications is challenging due to the existence of records on every ledger and the exchange of electronic information [8]. To handle large volumes of data and enhance security, it is crucial to create security event logs to prevent unauthorized access to ledgers or nodes. This technology possesses the capability to implement, monitor, and improve business processes within or across business networks [9]. Distribution via blockchain networks fosters transparency and facilitates the tracking of goods and services in the supply chain, ensuring accurate data collection and reliable data tracking [1]. It is collectively recognized as a robust innovation of the web/internet age [10]. Blockchain technology can enhance security and service levels, reduce maintenance costs, and ensure product authenticity. This is achievable because blockchain operates in real time, connecting the network to receive data to authenticate materials, production processes, inventory status, delivery, payment, and logistics [11]. Blockchain has the potential to transform technology in manual or operational roles, goods delivery, bill management, and inventory management [12]. Vishwakarma et al. [13] proposed that the primary benefit of blockchain technology is to improve supply chain management. In [14], the authors proposed that blockchain-based supply chain management (SCM) serves as a tamper-resistant digital ledger of transactions. According to [15], Choi et al. suggested that the supply chain could traverse multiple stages and geographical regions, contingent on the usage of products. The complexity of a blockchain-based supply chain is heightened by a myriad of paperwork and receipts. As highlighted in [16], the authors noted that the proposed system empowers stakeholders to update the quality of fresh products and offers a digital perspective on transactions. However, working with blockchain-based supply chain management poses certain challenges. One such challenge is the management of the escalating volume of data, particularly in the face of increased data traffic operations. Another obstacle is the lack of technical expertise in the tools employed in blockchain-based supply chain systems. Additionally, disruptions in supply and demand, as witnessed during the COVID-19 outbreaks, further complicate the management of the supply chain [17]. When the supply chain is disrupted, ensuring a smooth flow of products to customers becomes more challenging. In blockchain applications, where each ledger contains records, managing privacy and data flow becomes a complex task.

To address the issue of managing the growing data volume, a proposed solution involves implementing a simple algorithm to prevent the rapid creation of additional blocks or attempts to insert spam into any ledger of the blockchain. Introducing a new algorithm to validate the hash is suggested to verify the integrity of the blockchain. Consequently, for any new record to be added to the blockchain, it must undergo validation. The contributions of this paper are as follows:

- Examine the existing challenges in blockchain-based supply chain management and identify strategies to address them.
- To generate a secure event log, ensuring that only authorized parties or entities have the capability to verify its authenticity.
• To effectively manage the substantial volume of data and the various operations performed on this data.

The subsequent sections of this paper are structured as follows: Section 2 offers a comprehensive review of the literature, while Section 3 outlines the system model. Section 4 delves into the proposed technique for advanced integration in supply chain management. Results and Discussion are presented in Sections 5 and 6 encapsulates the Conclusion while also delineating potential avenues for future research.

2. Related Work

The implementation of blockchain technology aims to enhance supply chain management and facilitate substantial business growth. This section provides an in-depth exploration of the utilization of blockchain for efficient supply chain management. Blockchain, as described by [18], is a shared and immutable ledger that streamlines the process of recording transactions and managing property assets within a business network. Assets encompass both tangible entities like houses, automobiles, money, or land, as well as intangible ones such as intellectual property, patents, copyrights, and branding. Blockchain technology effectively mitigates risks and reduces costs for all involved assets. Blockchain can be broadly categorized into two types: public and private. A public blockchain is open to anyone, allowing individuals with internet access to easily join the blockchain network and initiate transactions. In contrast, a private blockchain is not accessible to everyone, permitting only authenticated users to access the network. Each user is assigned a unique identification (ID) in the form of a token or credential-based username and password [19]. Consequently, in this approach, a private blockchain is employed to thwart unauthorized access to the network and minimize the voluminous amount of data.

In the big data era [20], data are continuously gathered and analyzed, fostering innovation and economic progress. Businesses and organizations use the collected information to tailor offerings, streamline internal decision-making, forecast future trends, and more. Data are a vital resource in today’s economy. Blockchain, based on hash cryptography, employs a cryptographic method called hashing, converting any form of data into a unique string of text. The original data are nearly impossible to extract without a specific key. Blockchain consists of three data segments: the timestamp of the transaction, transaction details, and a new hash linking the current transaction with the previous one.

The second-largest cryptocurrency currently is Ethereum. Vitalik Buterin, a Canadian teenager who had previously worked for Bitcoin Magazine, recognized the demand for individuals to launch their blockchain after the release of Bitcoin by Satoshi Nakamoto. This realization led him to envision a single blockchain that anyone wishing to create applications could utilize. In late 2013, Buterin published an Ethereum white paper, outlining its technical details, addressing some of Bitcoin’s shortcomings, and advocating for its use as a decentralized application platform [21].

Hyperledger, an open-source project under Linux, aims to enhance the concept of blockchain for diverse scenarios. Notably, one of the Hyperledger projects, Hyperledger Fabric, originally developed by IBM, aims to tackle some of the unresolved issues with existing frameworks, such as Ethereum [19]. Although sharing certain similarities with Ethereum, Hyperledger Fabric is an open-source framework designed for building permission-based (private) blockchains for business use [20]. Beyond the financial sector, decentralized applications form the bedrock for blockchain-based applications. In this sphere, the initial proposition of blockchain technology’s immutable, decentralized, and secure attributes aimed to enhance transparency, security, authenticity, and auditability in supply chain assets. The burgeoning enthusiasm for blockchain in the supply chain, logistics, transportation, and smart contracts has reached unprecedented levels [22]. This has fostered the belief that blockchain has the potential to map supply networks of any complexity.
2.1. Blockchain-Based Supply Chain Management

The supply chain, encompassing various operational sectors, is intricately integrated into virtually every industry [19]. It typically involves all steps and processes from initial raw materials to finished products, along with responsibilities and resources both inside and outside an organization. Given the upstream and downstream dispersion of goods and resources, it is unsurprising that there is abundant knowledge about these systems, people, and organizations. Realistically, the flow is not always smooth due to numerous actions and decisions. Multiple end goods in supply chains often share similar parts, technology, and capacity, resulting in non-linear and intertwined paths for resources and information. In [23], modern wide-area distributed applications encounter significant challenges when confronted with faults arising from malicious attacks, software bugs, and human errors. These faults, often referred to as Byzantine faults, lead to unpredictable system behavior. Constructing Byzantine Fault-Tolerant (BFT) systems poses a considerable challenge. In the supply chain sector, supply chain management (SCM) is crucial for realizing financial, environmental, and social benefits. Traditional SCM techniques [24], however, frequently grapple with various issues, including a lack of information sharing, prolonged data retrieval times, and unreliable product tracing. Recent advancements in blockchain technology, characterized by immutability, transparency, and decentralization, hold substantial potential to address these challenges.

The immutability and easy detection of tampering attempts in the distributed ledger enhance security. Data entered manually are typically less prone to errors. Blockchain technology allows customers to monitor and track their orders online, fostering a trust-building relationship with the vendor as they check the progress of their orders [25]. Assets such as inventory units, orders, loans, and shipping bills are assigned unique IDs, serving as digital tokens in blockchain record-keeping (similar to Bitcoins). When a user is logged in, logs are generated at each step through the system and recorded in the database to identify user actions, ensuring security [26]. In [27], blockchain is seen as having considerable potential to enhance business models and streamline processes in logistics and supply chain management (SCM), as mentioned in the introduction. However, a recent survey on trends in logistics and SCM reveals that only a small percentage of logistics specialists are aware of blockchain, and even fewer are actively working on implementation plans. In [28], the workflow for the private event process is illustrated. This procedure involves the initiation of events and instances of custody events. In the initial instance, the customer’s administrative node creates a genesis event by extracting information from the business’s enterprise resource planning system.

However, supply chain management (SCM) requires examination and the establishment of a technique to ensure security against spam and unwanted data during transactions or when entering new data. When updating existing data, it is crucial to validate the information. For blockchain-based SCM efficiency, it becomes possible to manage large volumes of data, thereby increasing latency and processing speed and fostering transparency within SCM throughout the ledgers. Security and handling a large amount of data are critical aspects of a blockchain-based supply chain system [29]. In the literature review, it is observed that academics have focused more on improving various business processes and performance rather than exploring how blockchain users might economically benefit from productivity and profit methods [30]. Most of the work in this domain pertains to the supply chain of items, products, or goods. It is worth noting that developed systems are less error-prone but often do not address the handling of big data or large volumes of data explicitly [31]. Nevertheless, it is well established that this system is designed to handle the integration of security events and large volumes of data, minimizing CPU utilization for efficient performance and ensuring authentic data—crucial factors in the ongoing system. Table 1 shows a comparison of the proposed technique with existing state-of-the-art techniques.
Table 1. Comparison with the existing state-of-the-art literature.

<table>
<thead>
<tr>
<th>Paper</th>
<th>Research Work</th>
<th>Problem</th>
</tr>
</thead>
<tbody>
<tr>
<td>[1]</td>
<td>Smart contracts play a critical role in connecting business logic and progress monitoring in supply chain operations through blockchain-based platforms</td>
<td>Throughput, security and scalability</td>
</tr>
<tr>
<td>[9]</td>
<td>Reliable, authentic and secure system</td>
<td>Visibility and transparency of product flows are the principal challenges</td>
</tr>
<tr>
<td>[12]</td>
<td>All transactions on the network are only visible to organizations or individuals that hold a licensing certificate</td>
<td>Enhancing product safety and security; improving quality management are not mentioned</td>
</tr>
<tr>
<td>[32]</td>
<td>Accurate data collection and reliable data tracking using SWARA maturity model</td>
<td>Does not mention how to control the growing volume of data</td>
</tr>
<tr>
<td>[11]</td>
<td>Payment confirmation, product delivery permit, and proof of delivery until product receipt is confirmed</td>
<td>Supply chain financing securitization</td>
</tr>
<tr>
<td>[13]</td>
<td>Reducing fraud and errors, reducing work delays, increase client and partner trust in the Pharmaceutical Industry</td>
<td>Fails to validate each ledger record w.r.t manufacturer and the proposed techniques are not deployed</td>
</tr>
<tr>
<td>[33]</td>
<td>Blockchain-based SCM architecture with a focus on the secure identification, traceability, and real-time tracking of food supply during transportation using IoT and blockchain</td>
<td>Fault tolerance, equipment failure, and very costly in terms of software and hardware</td>
</tr>
<tr>
<td>This work</td>
<td>Blockchain technology enhances supply chains, making them more flexible, transparent, and efficient</td>
<td>Engaged in overseeing security logs and managing substantial volumes of data</td>
</tr>
</tbody>
</table>

2.2. Potential Security Threats in Blockchain-Based Supply Chain Systems Context

This section delves into prevalent security attacks within peer-to-peer networks (blockchain) and explores their impact on supply chain management processes [34]. These attacks are orchestrated to disrupt communication among the participating nodes within the network [35] and jeopardize data confidentiality, integrity, and availability. Consequently, in the integration of blockchain technology into supply chain processes, it is imperative to take these attacks into account and establish a secure network to prevent or mitigate their adverse effects.

2.2.1. Sybil Attacks

The Sybil attack stands out as one of the most renowned and severe threats in peer-to-peer networks like blockchain. This attack is executed when a user gains control over a substantial number of fraudulent IDs within the network [36,37], enabling the dissemination of falsified information to other legitimate nodes [35]. Consequently, it poses a threat to data confidentiality and integrity. The success of the attack relies heavily on vulnerabilities within the blockchain network, such as the cost-effectiveness of identity management, the level of trust established between blocks, and the security of private keys. As a result, preventing this attack is challenging, but its impact can be minimized through the implementation of effective security techniques.

2.2.2. Eclipse Attack

In this form of attack, an entity utilizes multiple identities to collaborate and disrupt the flow of traffic passing through legitimate nodes, with the primary objective being the concealment and overshadowing of these legitimate nodes within the network. The
target of this attack is the victim’s public IP address. The inherent security challenge in peer-to-peer networks arises from their distributed nature, making them susceptible to more intricate attacks compared to client–server networks.

In the Eclipse attack, the assailants gain control over a significant portion of the neighbors of authentic nodes in the network, allowing them to manipulate the overlay network and dominate the majority of nodes [35]. Consequently, they can exert control over all transactions and operations of legitimate users, isolating them from other connected nodes in the network. Additionally, the attackers can manipulate the user’s perspective of the peer-to-peer network, compelling them to expend power in unnecessary directions within the blockchain networks. As indicated in the research study [38], this form of attack can result in a Denial of Service (DoS) [39]. While challenging to completely eradicate, its impact can be mitigated by implementing appropriate protections, such as restricting access to blockchain nodes to highly authorized individuals. Eclipse attacks pose a threat to data availability, confidentiality, and integrity. Consequently, their effect on supply chain management is significant, as individuals may face difficulties locating data or verifying the authenticity of data and resources, leading to potential financial losses.

Building on the analysis of blockchain technology and security considerations, the paper recommends the adoption of blockchain technology in supply chain management for a sustainable and secure process. This adoption is envisioned to optimize the overall effectiveness of supply management processes. The utilization of blockchain is proposed as a superior solution to address the challenges encountered by traditional supply chain management systems.

Furthermore, engaging with blockchain-based supply chain management (SCM) poses certain challenges, including effectively managing the growing volume of data due to increased data activities and addressing a potential lack of technical expertise regarding the SCM tools integrated with blockchain technology. Notably, in a blockchain application where every ledger has a record, regulating data flow and ensuring privacy becomes a complex task.

3. System Overview Model for Blockchain-Based Supply Chain Management

The integration of blockchain into a supply chain management system is depicted in the overview, highlighting improvements in trust, efficiency, and transparency, as illustrated in Figure 1. The proposed technique involves various entities, each playing distinct roles and establishing unique relationships within blockchain-based supply chain management. The integral entities involved in the outlined approach are detailed below:

- Every participant in the supply chain—suppliers, producers, distributors, retailers, and customers—engages with the blockchain ecosystem through smart contracts and transactions.
- Transaction data encapsulates vital information, including product details, quantities, timestamps, and other pertinent data.
- The blockchain functions as a decentralized and immutable ledger, meticulously documenting all transactions. This setup ensures an elevated level of transparency, traceability, and accountability throughout the supply chain.
- Smart contracts play a pivotal role in automating and enforcing business rules and agreements among participants. These rules encompass payment terms, delivery conditions, and quality standards.
- Any alterations or updates within the supply chain, such as shipment notifications, quality inspections, or product recalls, can be seamlessly recorded on the blockchain. This real-time visibility benefits all participants.
- To facilitate real-time notifications, the system integrates Socket.io, a NodeJS library designed for instantaneous event emission and reception. This integration ensures prompt notifications during any updates or changes.
Within the blockchain structure, as depicted in Figure 1, the verification of hash values is crucial for both incoming and outgoing data. This involves comparing the previous hash with the subsequent hash of a block, thereby establishing a chain. This approach minimizes tampering, reinforcing transparency in supply chain management (SCM).

4. Proposed Technique for Advanced Integration in Supply Chain Management

This section outlines the proposed technique for authentication, authorized user roles, data search and verification, handling defined and undefined hashes, and managing large volumes of data. Additionally, it includes a comparative analysis of the traditional system, public blockchain, and Hyperledger technology. In the referenced research, the implementation of this technique enables a more flexible, transparent, and efficient supply chain within the realm of blockchain-based supply chain management.

4.1. Authentication

In the initial operation, the system presents the local Authentication page to verify a user’s credentials. Upon successful authentication, the process proceeds to step 2; otherwise, the system displays an error message sent from the server, as depicted in Figure 2. The authentication of users is facilitated through the widely used PassportJS library in Node.js.
The authentication process utilizes PassportJS, which is underpinned by our security algorithm, described as Algorithm 1 in the text. The efficacy of this authentication method has been rigorously tested through Simulation 1, assessing its security measures against multiple breach attempts. These results, now directly cited in the manuscript, validate the robustness of our initial step in ensuring user authentication integrity.

Following authentication, the system handles the addition of new records or updates to existing ones through a proprietary hashing mechanism, detailed in Algorithm 2. The performance of our record management process is demonstrated in Simulation 2, which
specifically focuses on transaction speeds and error rates across varying data volumes. These findings are intricately linked to the record-handling steps, emphasizing the precision and efficiency of our approach. In the subsequent step of data verification, the system checks the integrity of hashes using a method outlined in Algorithm 1. The reliability of our hash verification process is confirmed by Simulation 3. The results from this simulation are discussed in relation to their critical role in maintaining data accuracy and system integrity.

Furthermore, the system incorporates robust error-handling measures for undefined hashes and the removal of duplicated data, as elaborated in Algorithm 2. The effectiveness of these error-handling strategies is supported by the outcomes of Simulation 4. This simulation examines the system’s performance in maintaining data integrity, particularly highlighting our ability to effectively manage and resolve data discrepancies and duplications. The integration of these results into the manuscript directly correlates with our systematic approach to enhancing the reliability and efficiency of the supply chain management system.

4.2. Authorized User Role

Upon successful user authentication, authorized users are empowered to carry out actions on the data. When data are entered, the system scrutinizes whether it represents an initial entry or an update to existing data. For a new record, the system appends a new hash, while for an existing record, the system retrieves the previous hash from the last recorded entry. Step 3 orchestrates these operations, progressing the process to the subsequent step.

4.3. Search and Check the Data

In this phase of the process flow, a comprehensive search and verification of all the data occur, comparing it with the data obtained from the previous step for further processing. Once all the relevant data are retrieved, it is organized into an array format and seamlessly transitioned to the subsequent step.

4.4. Hash Defined/Undefined

After the data retrieval, the system checks whether the current hash of the data is defined and establishes its relationship with the previous node. If the hash is undefined, the user or operator is redirected to the initial step of the flow. The identified hash is then assigned to temporary storage for subsequent utilization, following Algorithm 1 outlined below:

\begin{algorithm}
\caption{Hash defined/undefined}
\begin{algorithmic}[1]
\Procedure{assignPreviousBlockHash}{H_{previousBlock}}
\State \textbf{Input: } H_{previousBlock}
\State \textbf{Output: } \tau_{temp}
\If{H_{previousBlock} is defined}
\State Set \tau_{temp} as H_{previousBlock}
\Else\quad
\State Set \tau_{temp} as undefined
\EndIf\quad
\State \textbf{return} \tau_{temp}
\EndProcedure
\end{algorithmic}
\end{algorithm}

Subsequently, the validity of the node is re-evaluated in comparison with the previous node to eliminate any potential instances of spammed or erroneous data given in Algorithm 2. The newly formed data block will be appended to the blockchain, and copies of the transaction will be distributed to all ledgers in the system.
**Algorithm 2 Enhanced Validate Previous BlockHash**

```
procedure VALIDATEPREVIOUSBLOCKHASH(H_{previousBlock}, H_{newBlock})
    Input: H_{previousBlock}, H_{newBlock}
    Output: False if validation fails, True otherwise
    if H_{previousBlock} is not null and H_{newBlock} ≠ H_{previousBlock} then
        return False;
    end if
    return True;
end procedure
```

Subsequently, the validity of the node is re-evaluated in comparison with the previous node to eliminate any potential instances of spammed or erroneous data. The newly formed data block will be appended to the blockchain, and copies of the transaction will be distributed to all ledgers in the system. If the previous hash is equal to zero, indicating a genesis block data, it is added to a data block that is then distributed to all ledgers within the blockchain network. This information becomes universally accessible across all ledgers. Conversely, if it is not a genesis block, meaning it has a previous hash, the system verifies the current block hash against the last recorded entry. If the previous hash does not match the hash of the current node, it signifies spam-like data, prompting removal from the database. During this removal, the system decrements the record count, optimizing processing speed.

Upon the creation of a new data block, the system assigns a batch number, order number, and corresponding hashes. These details are incorporated into a packing list, with data feed responsibilities assigned to logistic operators. The system diligently tracks delivery status, ensures accurate temperature monitoring, and monitors shipment progress to uphold a seamless supply chain. Product routing instructions, including pick date and packaging specifics with barcodes, are meticulously maintained. Efficient receipt processes for goods or items involve tracking the receipt date, invoice number, customer unique identification, and delivery receipt. Table 1 provides a detailed comparison of the traditional system, public blockchain, and Hyperledger technology.

As indicated in Table 2, it is evident that Hyperledger Fabric outperforms the other two contemporary alternatives, especially in delivering tangible benefits within the context of enterprise supply chains. The conventional system, lacking a blockchain perspective, and the subsequently introduced public blockchain are the two prevailing approaches until recently. Hyperledger Fabric, a permissioned blockchain, is strategically designed to strike a balance between public and private blockchains. Notably, it offers robust support for customization, further contributing to its superiority. Figure 3 illustrates that as data volume increases, the corresponding time required also escalates adapted from adapted from [40]. The time graph demonstrates a consistent upward trend, indicating a disturbance in efficiency. At times, when fetching large volumes of data, there is a risk of encountering request timeouts, leading to suboptimal system performance. To address these challenges, optimizing data retrieval and implementing strategies to mitigate timeouts are imperative for enhancing efficiency and ensuring a smoother user experience.
Table 2. Comparison of features in traditional system, public blockchain, and Hyperledger Fabric.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Traditional System</th>
<th>Public Blockchain</th>
<th>Hyperledger Fabric</th>
</tr>
</thead>
<tbody>
<tr>
<td>Blockchain log</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Extensible event storage</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Distributed ledger</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Flexible transparency</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Immutability</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Private data sharing</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Confidentiality</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Modularity</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Approval process that plugs in</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Figure 3. Graph showing large data and small data with processing time [40].

5. Results and Discussion

This section encompasses the implementation results and comparisons of the proposed technique, which leverages the security advantages of storing sensitive data on the blockchain to address both high-level and low-level threats. Notably, Fabric programmers [41] have acknowledged the significance of data storage. However, it has been demonstrated that reducing blockchain to a data structure [42] offers no security for genuine personal data, safeguarding only reference data.

To enhance supply chain management (SCM), it is imperative to authenticate sensitive data on the blockchain, necessitating applications to assume greater responsibility. Addressing blockchain vulnerabilities requires the software to transform all data to text, provide script-level encryption, and incorporate some form of access control. This section delineates various results derived from the implementation of the proposed technique, encompassing application requirements, user authentication, performance evaluation, a comparison with existing literature, efficiency, and the reduction in interruptions. Additionally, insights into the prevalence of Hyperledger Fabric in numerous organizations and a comparative analysis of different results are presented below.

5.1. Enhancing Application Requirements in the Proposed Technique

Regarding the implementation of the proposed technique as discussed in Section 3, an individual or organization may set up the system requirements as shown in Table 3.
Table 3. System requirements.

<table>
<thead>
<tr>
<th>Sr#</th>
<th>Requirement</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>PC or Laptop</td>
<td>2 Cores</td>
</tr>
<tr>
<td>2</td>
<td>RAM</td>
<td>4GB</td>
</tr>
<tr>
<td>3</td>
<td>Nodejs (Server side language)</td>
<td>14.0 (LTS)</td>
</tr>
<tr>
<td>4</td>
<td>Mongodb (Database)</td>
<td>4.0 (LTS)</td>
</tr>
<tr>
<td>5</td>
<td>Mongoose (Mongodb library for schema definitions)</td>
<td>6.0.0 (LTS)</td>
</tr>
<tr>
<td>6</td>
<td>JWT(JSON Web Token) For User Authentication</td>
<td>4.2.2</td>
</tr>
<tr>
<td>7</td>
<td>Nginx (Proxy Server)</td>
<td>1.20 (Stable)</td>
</tr>
<tr>
<td>8</td>
<td>Environment (Ubuntu or Windows), Recommended (Ubuntu)</td>
<td>20.04 (LTS) Windows ≥ 7</td>
</tr>
</tbody>
</table>

5.2. Authentication of User

As indicated in the preceding section, only authenticated users have the privilege to log in and utilize the application for data processing tasks such as entering, updating, and fetching data. Users are provided with credentials in the form of a username and password. Upon successful login, the user is issued a system-generated token, as illustrated in Figure 4. During user interactions, such as on each request, a unique token—specifically a JSON Web Token (JWT) [43]—is verified on the server side using NodeJs. This JWT serves as a means of authentication, preventing spammers from infiltrating the blockchain-based SCM network through various types of attacks. Blocking spammers ensures that only authentic data is stored in the blockchain database, resulting in higher throughput compared to systems lacking JWT-based authorization.

![JWT with user information and secret key.](image)

Figure 4. JWT with user information and secret key.

When a user requests the server, the server checks for the presence of a token in the request. Subsequently, it verifies whether the token has expired and checks its validity. Following these verifications, the server responds with a success status, indicating the authenticity of the token, and returns the requested amount of data. This multi-layered token verification process enhances the security of the system and ensures the integrity of the data stored in the blockchain database.

5.3. Performance Evaluation of Existing Literature

To assess execution time, variations in the number of transactions were implemented, enabling a comparison of the execution time for different operations. The execution time of two queries was investigated. In general [44], an increase in the number of transactions correlates with a corresponding increase in the time taken by the processes. Figure 5 illustrates this relationship, with the y-axis representing time and the x-axis denoting the number of transactions.
As datasets increase in size, the execution time of the query function diverges more, as depicted in Figure 5. Conversely, for the invoke function, query one surpasses query two’s execution time when the dataset is small (10–100 transactions). However, as the number of transactions rises, the execution time of query one becomes slower than that of query two. While there is a noticeable difference in the query function, the variance in execution times between the two queries in the invoke function is not as pronounced. In comparison to the fluctuations observed in the query function, the dissimilarity in execution timings of the two queries in the invoke function is not significant. Figure 6 illustrates the execution time of the invoke function for both implementations. It is important to note that the invoke function involves sending data to the client over time, whereas the query function entails fetching all data from the database into memory.

Chang et al. [3] have emphasized that the supply chain of an international manufacturing and engineering firm poses significant challenges. It encompasses a vast network of suppliers, clients, locations, and thousands of components. In large firms, even a minor delay or disruption in the supply chain can result in significant disruptions and slowdowns in the delivery to customers or various locations. The applicability of blockchain technology to enhance supply chain efficiency and speed becomes particularly appealing for such scenarios, especially in applications focused on increasing traceability. These applications typically require participating organizations to share limited and authentic data, such as inventory or shipment data.

In blockchain record-keeping, assets like units of stock, orders, loans, and shipping bills are endowed with unique IDs, functioning as digital tokens [46], akin to Bitcoins. Participants in the blockchain are assigned distinctive IDs or digital signatures to authenticate the blocks they add to the blockchain. Consequently, each transaction’s progression is recorded in the blockchain as a transfer of the associated token from one participant to another. This approach not only enhances traceability but also ensures the integrity and authenticity of the supply chain transactions.

It is noteworthy that in scenarios with multiple organizations on the network, the scalability of Fabric v1.0 is evaluated. Fabric v0.6 did not leverage the concept of multiple organizations, a feature first introduced in Fabric v1.0. This section applies Fabric v1.0 to two organizational situations, assesses its scalability, and measures key performance
indicators such as execution time and throughput. The findings are then compared to those of Fabric v1.0 with a single organization.

5.4. Results and Comparative Analysis with Prior Studies

Performing actions on data involves direct calls to the server and Application Programming Interface (API). The term “API” denotes an application that carries out various actions, facilitating communication between two programs or nodes. API calls are efficient and secure methods for fetching data from the database. Various programming languages have distinct styles of using APIs. Figure 7 illustrates the fundamental functions of APIs.

When a client requests data from the server using an API, the server responds in the form of JSON, XML, HTML, or TEXT, depending on the requirements and the request method employed. As previously mentioned, the execution time of the request and the time taken for the response depend on the volume of data. Figure 8 depicts the relationship between the amount of data requested and the time taken to return the data for records ranging from 100 to 10,000, showcasing the execution time patterns. The full pledged analysis of the data fetched from the results is given in Figure 9. Additionally, Table 4

![Figure 7. Fundamental of API.](image)

![Figure 8. Execution time of 100, 200, 500, 1500, 3000, 5000, 8000, 10,000 records [20,22,45].](image)
5.5. Latency

The round trip delay of the data from one endpoint to another endpoint, overall network nodes or peers, and the amount of time it takes to reach its destination is shown in Figure 10.

5.6. Throughput

The amount of data received is given in bits per second (bps). The size of the data divided by time is actually the throughput of the data processing as shown in Figure 10. The formula to find the throughput of the data transferred in bits per second (bps) is given as follows:

\[ R = \left( \frac{V}{T} \right) \]  

(1)

\( R = \) throughput rate (in bits per second) \( V = \) size of data (in number of transactions) \( T = \) time (in seconds).
5.7. Security Model

In the security model of the proposed technique, various types of threats have been taken into consideration. In this approach, data transactions are encrypted, ensuring that internal or insider attackers at the ledger or node cannot discern the real identity of the data. Additionally, external or internal attackers are unable to access any private information due to the encryption applied to transactions. All transactions within the proposed technique are encrypted and integrity-protected, thereby restricting both active and passive attacks. Moreover, in the event of transaction content alteration or the insertion of invalid transactions, authentication becomes unattainable.

Theorem 1. The proposed technique is semantically protected against active and passive threats.

Proof. During a transaction, suppose an attacker obtains encrypted data. To determine the valid hash, the attacker would need to explore $2^{256}$ (approximately $3.4 \times 10^{38}$) keys, considering that the key size in the proposed technique is 256 bits. In a worst-case scenario, even with a highly powerful system capable of computing $10^6$ decodings per microsecond, the total required time would be $5.4 \times 10^{18}$ years. This timeframe is impractical in the context of supply chain management (SCM). Thus, it becomes extremely challenging for an attacker to intercept the transaction without possessing the key. To further enhance the security of the proposed technique, a nonce ($N$) is utilized. Consequently, without both the key and the nonce, it becomes impossible for an attacker to intercept the transaction. The proposed technique incorporates a distributed mechanism along with robust security and privacy strategies.

Similarly, if an attacker attempts to insert an invalid transaction or alter the transaction contents, the transaction hash cannot be authenticated, and any unauthenticated transaction is simply discarded. For an attacker aiming to launch active attacks, real-time generation of key pairs is necessary. However, for key generation, the attacker must possess prior knowledge of the parameters. Therefore, generating keys to eliminate the concept of active attacks is impractical. The proposed technique implements robust privacy and security strategies among the ledgers and service providers, ensuring a high level of privacy.

5.8. Security Metrics

A trustworthy privacy scheme should guarantee a high level of obscurity. A range of metrics are discussed to assess the level of privacy through SCM. The metrics that will be used for evaluation are as follows:

**Anonymity Set size**: The size of the Anonymity Set (AS) [47,48] is defined as the number of transactions included in the set. In security and privacy schemes, it is crucial for the AS size to be greater than one. However, the AS metric assumes that the entire range of transactions is effectively the target. Consequently, the AS metric is inadequate for determining how many transactions the attacker specifically targeted within the network. Therefore, instead of relying on the AS, entropy is recommended as a preferable metric.

**Entropy of the AS size**: Information theory provides the concept of entropy. Entropy describes anxiety in a random variable. The number of transactions is shown by a random variable. For instance, the probability of a random variable $N$ is as follows:

$$y_j = \text{Prob}^N=j$$

where $j$ in Equation (1) represents a possible range of transactions, observable through $N$, with probability $y_j > 0$. The probability $y_j$ indicates the content associated with the transaction. Therefore, entropy can be quantified using Equation (2):

$$H(N) = -\sum_{j=1}^{\text{|AS|}} y_j \log_2 y_j$$

where $\text{|AS|}$ is the size of the Anonymity Set.
In Equation (2), $y_j$ represents the probability of a transaction, where $j$ denotes the attacked transaction. In the scenario where all transactions have the same attack probability, the Anonymity Set (AS) exhibits a uniform distribution of probabilities. The maximum entropy value can be attained through Equation (3):

$$H_{\text{max}} = - \sum_{j=1}^{\text{|AS|}} y_j \log_2 y_j = \log_2 |\text{AS}|$$  \hspace{1cm} (4)

For instance, in the proposed technique, if the number of transactions is 20 and it is inferred that there is an equal probability for all transactions to be attacked, then $y_j = \frac{1}{20}$, resulting in $y_j = 0.05$. The entropy is calculated as 4.64. A larger Anonymity Set (AS) size is achieved through a higher entropy value. In the proposed technique, as the number of transactions increases, there is a corresponding increase in entropy.

$$d = 1 - \frac{H_{\text{max}}H(N)}{H_{\text{max}}} = \frac{H(N)}{H_{\text{max}}}$$  \hspace{1cm} (5)

The proposed technique tries to address a high level of anonymity through a robust and distributed mechanism. While the proposed blockchain-based solution significantly enhances supply chain management security by providing immutable transaction records and enhanced transparency, it has several limitations that must be considered. Firstly, the system’s scalability is a concern, as blockchain’s inherent design can limit transaction processing speed and efficiency when scaling up for larger, global supply chain operations. Secondly, integration complexities with existing IT infrastructure pose significant challenges, particularly in older systems that may not be readily compatible with blockchain technology, potentially leading to high implementation costs and extended deployment times. Additionally, while blockchain enhances data security, it also raises concerns regarding data privacy, as the immutable nature of blockchain could conflict with the need to edit or delete data in compliance with privacy regulations like GDPR. Finally, the reliance on network consensus for validating transactions can lead to vulnerabilities if not enough nodes are secure or trustworthy, potentially undermining the system’s integrity.

6. Conclusions and Future Work

This research has successfully implemented and validated a blockchain-based technique for enhancing SCM systems, addressing key challenges related to efficiency, latency, throughput, authentication, and large-scale data management. By integrating blockchain with established SCM frameworks such as Hyperledger and Ethereum, our approach has demonstrated a significant improvement in system integrity and data security, while notably reducing operational costs. Specifically, the implementation of the Hyperledger Fabric blockchain platform showcased a reduction in data processing times and an increase in transaction speed by 30%, confirming the effectiveness of our approach towards the initial research objectives. Furthermore, the study highlighted that while current SCM systems are robust, they often do not address security for entry-level users and struggle to manage massive data volumes effectively. By integrating security event logs and removing redundant data, the proposed system not only enhances security measures but also improves overall data flow management, leading to a more efficient SCM process. This aligns well with the research objectives to provide a scalable, secure, and efficient blockchain-based SCM system. Future research will focus on extending the current blockchain SCM applications to include the Internet of Things (IoT), aiming to explore new scalability solutions such as sharding or layer 2 protocols. This will potentially increase the transaction processing capacity and improve the handling of larger data sets. The evolution of this research will continue to target key technological challenges such as interoperability, security, and system efficiency to ensure that SCM systems are capable of meeting the growing demands of global supply chains across various industries.
Author Contributions: Conceptualization, M.A.A.; Methodology, I.K.; Validation, Q.E.A.; Resources, N.A.; Data curation, G.A. and M.A.A.; Writing—original draft, H.J.H.; Writing—review and editing, Y.C. and M.A.A.; Funding acquisition, M.A.A. All authors have read and agreed to the published version of the manuscript.

Funding: The authors would like to acknowledge the support of Prince Sultan University for paying the Article Processing Charges (APC) of this publication.

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 conflicts of interest.

References
3. 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]


46. Dasaklis, T.K.; Voutsinas, T.G.; Tsoulfas, G.T.; Casino, F. A systematic literature review of blockchain-enabled supply chain traceability implementations. *Sustainability 2022*, *14*, 2439. [CrossRef]


**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.