

A cyber-physical system with blockchain integrated chaotic secure hash algorithms-256 for secured supply chain management system

K. R. Praneeth *

School of Management

The Apollo University

Chittoor 517127

Andhra Pradesh

India

Hayder M. A. Ghanimi [†]

Department of Information Technology

College of Science

University of Warith Al-Anbiyaa

Karbala 5751

Iraq

and

Department of Computer Science

College of Computer Science and Information Technology

University of Kerbala

Karbala 5751

Iraq

M. Srinivasa Narayana [§]

Department of Centre for Distance and Online Education

Koneru Lakshmaiah Education Foundation

Vaddeswaram 522302

Andhra Pradesh

India

* E-mail: dr.praneeth@apollouniversity.edu.in (Corresponding Author)

[†] E-mail: hayder.alghanami@uowa.edu.iq

[§] E-mail: dr.srinivasanarayana@gmail.com

Kafila [†]
School of Business
SR University
Warangal 506371
Telangana
India

Sireesha Nanduri [@]
Faculty of Management Studies
CMS Business School
JAIN (Deemed-to-be University)
Bengaluru 560009
Karnataka
India

Ravi Kumar Bommiseti [#]
Department of Commerce
Akal University
Talwandi Sabo
Bathinda 151302
Punjab
India

Sudhakar Sengan ^{\$}
Department of Computer Science and Engineering
PSN College of Engineering and Technology
Tirunelveli 627152
Tamil Nadu
India

Pankaj Dadheech [^]
Department of Computer Science and Engineering
Swami Keshvanand Institute of Technology, Management & Gramothan (SKIT)
Jaipur 302017
Rajasthan
India

Abstract

In the background of the contemporary Supply Chain (SC) environment, the motivation is on cyber security of Cyber-Physical Systems (CPS), openness, and optimization. This

[†] E-mail: kafila@sru.edu.in

[@] E-mail: drnsireesha.iimb@gmail.com

[#] E-mail: ravi9949418650@yahoo.com

^{\$} E-mail: sudhasengan@gmail.com

[^] E-mail: pankajdadheech777@gmail.com

paper aims to develop a Secured Supply Chain Management System (SSMS) that combines Blockchain with Chaotic Secure Hash Algorithm-256 (CPS + BC + Chaotic SHA-256) encryption. BC is a distributed and secure database that can be used to track the measure of goods in real-time and with digital certification. Chaotic SHA-256 is used to enhance security by integrating chaotic systems into the SHA-256 Hash Function (HF), thereby increasing the layers of unpredictability and security against attacks. Besides improving the quality of transaction records, this method also provides the best defense against data theft and fraud. The developed CPS + BC + Chaotic SHA-256 has the potential to overcome most of the problems that affect the SC, such as counterfeits and organizational inefficiencies, by utilizing Smart Contracts (SC). The combination of BC in and the Chaotic SHA-256 (C- SHA-256) algorithm generally enhances security and SC stability.

Subject Classification: 93E10, 94A13.

Keywords: Blockchain, Security, Privacy, Chaotic algorithm, Supply chain, SHA 256.

1. Introduction

Supply Chain Management (SCM) is essential today because it encompasses all the activities of providing consumer products and services. The protean nature of Supply Chain (SC) networks, in the context of global operations, combined with the constantly rising expectations for greater openness, speed, and safety, has called for more radical solutions [1]. Some (primary) problems associated with traditional SCM include increased incidence of fraud, lack of transparency, increased incidences of inefficiencies, and lack of traceability of products. To tackle these challenges, the solution of Blockchain (BC) has emerged, enabling the development of a decentralized and Secure Supply Chain Management System (SSCMS) [2]. BC generates a distributed ledger that can securely store every single transaction. This feature has become increasingly beneficial for SCM, as all SC network members can now track data [3]. The blocks in the BC have a record of the hash of the prior block's hash. This immutability ensures that once a transaction is completed and recorded, it cannot be altered, thereby preventing fake actions.

Applied to the SCM, BC allows for tracking and validation of products in the SC networks in real-time [4-5]. Manufacturers, suppliers, and retailers of products can all visit the BC to authenticate the products and their sources. This also helps ensure accountability, and in the event of any concerns, such as fake products or discrepancies in delivery, it is easy to identify them [6]. BC again enriches SCM with the SC feature, which enables the execution of tasks and the implementation of Smart Contracts (SC). SC contracts between consumers are becoming increasingly automated, with contract terms being coded. They perform and enforce contractual provisions whenever conditions are satisfied; they are not intermediary devices and avoid faults and time wastage. BC

technology integration in SSCMS also facilitates data collection and utilization for improvement. The information described to the BC is immediately available and can be interrogated to recognize SC and process performance or to identify problems that need fixing [7]. An SSCMS utilizing BC effectively addresses the problems that accompany traditional systems. It has been identified that BC improves the SC's security, credibility, and effectiveness by contributing an open, transparent, and automated system that can improve the SCN [8]. The remainder of the article is organized as follows: the summary of SCM + BC is detailed in Section 1, the complete study of literature is discoursed in Section 2, the proposed CPS + BC + Chaotic SHA-256 based C-SHA-256 is specified in Section 3, the result and discussion is proved in Section 4, and the article is concluded in Section 5.

2. Related Works

This chapter presents and describes different outcomes and reference approaches in using BC in the SC. It is based on applying Distributed Ledger Technology (DLT), SC, case studies, and integration with new technologies to improve the SC's traceability, transparency, and security. However, these advancements enhance SC efficiency and security; these difficulties are complexity, scalability, and immaturity. Table. 1 depicts the details of the recent studies directed at the application of BC in the SCM and the chances and problems realized by the application. The works discussed here prove how the BC mitigates significant problems typical of conventional SC, including opacity, vulnerability to fraud, and lack of traceability. BC is noted to propose security benefits, providing a clear and fixed record of transactions for the SC, inventory, and combating fraud. It describes use cases such as SC and product provenance while accepting some risks associated with BC implementation. Another case is the automotive industry, where the focus is on signifying that BC can help aggregate product data, enhance transactions, and enhance the dependability of SC. However, it recognizes problems such as technology inexperience, absence of well-defined best practices, and legal uncertainties as factors preventing BC from attaining broader acceptance. In [11], BC can enhance the SC through automation, scalability, and addressing legal challenges using Walmart and IBM's TradeLens. It also claims that clarity and efficiency have improved; however, it raises concerns about scalability and legalization. Authors discuss the integration of BC + NFT, along with double protection layers, to prevent counterfeiting and theft, demonstrating that the design of this CSP is compact. However, if extended to other parts of the hospital or other hospitals, it could prove challenging for the tool to function effectively. Altogether, these works demonstrate that BC can transform SCM; however, they also reveal that BC and its regulation present specific issues that need to be addressed.

Table 1
Comprehensive Analysis of SCMS

Outcome and Reference	Technique Used	Significance	Drawback
BC enhances SC traceability, transparency, and security [8].	(DLT), SC	Enhances traceability, optimizes inventory, prevents counterfeit products, and facilitates automated payments in SC.	The complexity of implementation and potential resistance from existing systems.
BC enhances product information aggregation, transaction security, and SC reliability [9].	Case studies, TOE Model	Reduces process costs, ensures product quality, and enhances visibility and digitization in the automotive SCM.	Technology naivety, lack of industry ethics, non-cooperation, and judicial uncertainty.
BC increases transparency and traceability in SCM, with applications in various industries [10].	BC Integration, Case Studies (Walmart, Maersk & IBM TradeLens)	Enhances SC clarity, efficiency, and integration with emerging technologies.	Scalability problems and challenges in conforming to legal frameworks.
The CSP reduces costs, improves transparency, and enhances SSCMS [11].	Non-fungible tokens (NFT), Holographic Labels, RFID, Private BC	It enables a secure and transparent method to verify product integrity, thereby incentivizing user trust.	Potential complexity in system setup and scalability and reliance on accurate integration of several technologies.

3. Proposed CPS + BC + Chaotic SHA-256 for SCM

The proposed CPS + BC + Chaotic SHA-256 security in SCM addresses key problems of transparency, efficiency, and robustness against attacks. The recommended CPS leverages BC's permanent ledger to provide a distributed, permanent record of transactions, enabling the verification and tracking of products in real-time. Chaotic SHA-256 further enhances security by incorporating chaotic sequences into the SHA-256 Hash Function (HF), thereby increasing unpredictability and resistance to cryptographic attacks. In this hybrid model, each transaction T_i is represented by a tuple (T_i, H_i, P_i) where $S_i \rightarrow$ transaction data, $H_i \rightarrow$ hash of the transaction and $P_i \rightarrow$ hash of the previous block. The Hash Function (HF) maintains the ledger's integrity, ensuring that any tampering alters. ' H_i ', invalidating the subsequent blocks. Chaotic SHA-256 modifies the SHA-256 function by incorporating chaotic sequences ' $C(t)$ ', Eq. (1).

$$H = \text{SHA256}(D \oplus C(t)) \quad (1)$$

where $DDD \rightarrow$ the transaction data, $C(t) \rightarrow$ the chaotic sequence generated at the time ' t '. This method increases the hash function's complexity and sensitivity to changes in ' $C(t)$ ', thus enhancing security.

Performance is evaluated using metrics like transaction Network Throughput (NT) (T_{NT}), which is the number of transactions processed per unit of time, and End-to-End Delay (EED) (L), the time taken from transaction initiation to inclusion in the BC, Eq. (2) and Eq. (3).

$$T_{NT} = \frac{N_{NT}}{T_{Total}} \quad (2)$$

$$L = T_{Confirmation} - T_{Initiation} \quad (3)$$

Security resilience (R) measures the system's resistance to attacks, as defined in Eq. (4).

$$R = 1 - P_{attack} \quad (4)$$

where $P_{attack} \rightarrow$ the probability of a successful attack.

Testing involves simulating several attack scenarios to assess P_{attack} and verify that R meets security standards. The simulation uses hardware with multiple nodes and BC platforms integrated with Chaotic SHA-256. Performance metrics are collected and analyzed to optimize system parameters, balancing performance (minimizing EED and maximizing NT) with security. Chaotic sequences can be generated using the logistic map in Eq. (5).

$$x_{n+1} = rx_n(1 - x_n) \quad (5)$$

where $x_n \rightarrow$ the current value; $r \rightarrow$ is a parameter controlling chaos. The sensitivity of Chaotic SHA-256 is evaluated using the differential avalanche effect in Eq. (6).

$$\Delta H = \text{SHA} - 256(D_1 \oplus C(t)) - \text{SHA} - 256(D_2 \oplus C(t)) \quad (6)$$

where $D_1, D_2 \rightarrow$ variable inputs, ensuring that minor deviations lead to knowingly variable hashes. SC automates tasks such as transaction verification and record updating, as shown in Eq. (7).

$$E_{contract} = \frac{T_{execution}}{N_{transaction}} \quad (7)$$

where $T_{execution}$ is the total execution time. This approach enhances the transparency and automation of the SCMS, addressing challenges such as forgery and inefficiencies by utilizing a robust and secure model (Algorithm 1).

Algorithm 1: C-SHA 256 for SCM

- Step 1.** For $i = 1$ to N
- Step 2.** Generate T_i
- Step 3.** Compute $H_i = \text{SHA-256}(D_i \oplus C(t))$
- Step 4.** Set $P_i = H_{i-1}$
- Step 5.** If tampering is detected in H_i
- Step 6.** Invalidate all subsequent blocks

- Step 7.** End If
- Step 8.** Compute $T_{NT} = \frac{N_{NT}}{T_{total}}$
- Step 9.** Compute $L = T_{confirmation} - T_{initiation}$
- Step 10.** Simulate attack scenarios
- Step 11.** Computed Pattack = Probability of a successful attack
- Step 12.** Compute $R = 1 - P_{attack}$
- Step 13.** For Each Chaotic Sequence $C(t)$
- Step 14.** Generate $x_{n+1} = rx_n(1 - x_n)$
- Step 15.** Update $H_i = \text{SHA-256}(D_i \oplus C(t))$
- Step 16.** End For
- Step 17.** Compute $\Delta H = \text{SHA} - 256(D_1 \oplus C(t)) - \text{SHA} - 256(D_2 \oplus C(t))$
- Step 18.** Ensure minor differences in inputs (D_1 , D_2) generate significantly different hashes
- Step 19.** Execute SC for transaction T_i
- Step 20.** Compute $E_{contract} = \frac{T_{execution}}{N_{transaction}}$
- Step 21.** Collect and analyze performance metrics (T_{NT} , L , R)
- Step 22.** Optimize system parameters to balance performance and security
- Step 23.** End For

4. Result and Discussion

Due to the SSCMS simulation, the hardware setup involves a multi-node network with servers and workstations that possess high-performance CPUs and sufficient RAM for BC processing. Another element of the node setup is to install a BC platform that can be HF, Ethereum, or another. In the case of the Chaotic SHA-256 implementation, a cryptographic library that supports the selected platform of the BC implementation is included. These are network simulators used in modelling different SC performances and monitoring tools used to evaluate the efficiency and security of the CSP. This setup ensures comprehensive testing of BC integration of cryptographic improvements. The parameters used to assess the effectiveness of an SSCMS that incorporates CPS + BC + Chaotic SHA-256 include the number of transactions processed per unit of time, the time taken, and the security model. Transaction NT refers to the number of transactions completed in one second, thereby quantifying the system's ability to support a massive volume of messages containing SC data (Figure 1). EED can be defined as the time it takes for a transaction to be validated on the BC, which determines the real-time tracking and responsiveness of the SC processes. The NT and EED are given in Eqs. (2) and (3). NT and EED are two critical measures that can be used to assess the effectiveness of SSCMS, particularly when using BC and Chaotic SHA-256. NT measures the CPS's ability to support transactions per second, abbreviated as TPS. A higher NT means the system can handle a large volume of SC data, requiring the system to run at high speeds and capacity. In this comparison, C-SHA-256 has a higher NT, which indicates that it was designed for high NT in high-traffic scenarios. At the same time, EED quantifies the time it takes to start a

transaction and has the information reflected on the BC. Reduced EED is crucial, particularly in terms of tracking and response times in SCM. The integration of C-SHA-256 has improved security but reduced the EED compared to other traditional systems, such as the TOE and DLT. This minimizes the EED of the CSP, providing almost instant verification and update of the information, which is critical for SCM's effective operation (Figure 2).

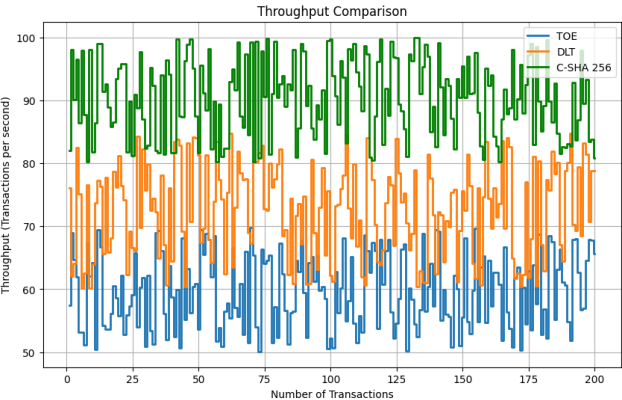


Figure 1
Comparison of NT

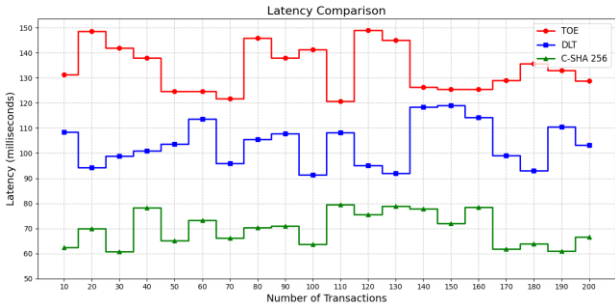


Figure 2
Comparison of EED

5. Conclusion and Future Work

Integrating the CPS + BC + Chaotic SHA-256 is the perfect solution for SSCM. BC helps maintain records and validate products, and Chaotic SHA-256 enhances the randomness of the hash. Some risks that may be incurred include counterfeiting, fraud, and data breaches; however, this system provides a more secure and efficient SCM solution. Besides improving data credibility using BC and the integration of Chaotic SHA-256, SC also helps increase the effectiveness of SC activities. Thus, this solution addresses the critical challenges of modern CS and opens the door to improved security and

management. For future work, it is possible to consider extending the proposed solution to utilize AI for predictive analytics and its application in real-time decision-making, thereby mitigating the system's rigidity in response to the dynamic nature of the SCM environment.

References

- [1] S. Saberi, M. Kouhizadeh, J. Sarkis and L. Shen, "Blockchain technology and its relationships to sustainable supply chain management," *International Journal of Production Research*, vol. 57, no. 7, p. 2117-2135, (2019).
- [2] M. M. Queiroz, R. Telles and S. H. Bonilla, "Blockchain and supply chain management integration: a systematic review of the literature," *Supply Chain Management: An International Journal*, vol. 25, no. 2, p. 241-254, (2020).
- [3] A. Gurtu and J. Johnny, "Potential of blockchain technology in supply chain management: a literature review," *International Journal of Physical Distribution & Logistics Management*, vol. 49, no. 9, p. 881-900, (2019).
- [4] R. Cole, M. Stevenson and J. Aitken, "Blockchain technology: implications for operations and supply chain management," *Supply Chain Management: An International Journal*, vol. 24, no. 4, p. 469-483, (2019).
- [5] S. Vijayarani, V. J. Tharini and C. Sivamathi, "Business intelligence for evaluating the intangible benefits of on-shelf high utility itemset from the temporal transaction database," *International Journal of Engineering and Advanced Technology*, vol. 8, no. 6, (2019).
- [6] G. Narayanan, I. Cvitić, D. Peraković and S. P. Raja, "Role of blockchain technology in supply chain management," *IEEE Access*, (2024).
- [7] M. A. Ghanimi, Hayder, P. Melgarejo-Bolivar, Romel, A. Tumi-Figueroa, S. Ray, D. Pankaj and S. Sudhakar, "Merkle-Damgård; RD hash functions and blockchains: Securing electronic health records," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 27, no. 2-A, p. 237-248, (2024).
- [8] M. A. Ghanimi, Hayder, T. Gopalakrishnan, D. G. Joel Sunny, K. Amarendra, D. Pankaj and S. Sudhakar, "Chebyshev polynomial approximation in CNN for zero-knowledge encrypted data analysis," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 27, no. 2-A, p. 203-214, (2024).

- [9] P. Vidya Sagar, M. A. Hayder, L. Prabhu Arokia Jesu Raja, D. Pankaj and S. Sudhakar, "Secure multi-party computation in deep learning: Enhancing privacy in distributed neural networks," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 27, no. 2-A, p. 249–259, (2024).
- [10] G. R. K. Rao, M. A. Ghanimi, Hayder, V. Ramachandran, D. Al-Qahani, D. Pankaj and S. Sudhakar, "Enhanced security in federated learning by integrating homomorphic encryption for privacy-protected, collaborative model training," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 27, no. 2-A, p. 361–370, (2024).
- [11] K. R. Jaya, T. Gopalakrishnan, M. Divyapushpalakshmi, K. Amarendra, D. Pankaj, S. Sudhakar, "Security and privacy concerns in social networks mathematically modified metaheuristic-based approach," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 27, no. 2-A, p. 371–382, (2024).

Received November, 2024