Library Progress International
Vol.44 No. 3, Jul-Dec 2024: P.1620-1627

Print version ISSN 0970 1052
Online version ISSN 2320 317X

Original Article

Available online at www.bpasjournals.com

Securing the Supply Chain: Leveraging IoT and Blockchain for FinancialRisk Management

[1]Dr.Deepesh Tiwari, [2]CFA Rakesh Gupta, [3]Unnati Agarwal, [4]Divya Tiwari, [5]CA AbhinavGaur, [6]Sundarapandiyan Natarajan,

[1,] Associate Professor, Department of Management,
Invertis University, Bareilly, Uttar Pradesh, India, deepeshtiwari709@gmail.com
[2]Assistant Professor,
Faculty of Management(MBA),
Invertis University, Bareilly,Uttar Pradesh, India, rakeshguptacfa@gmail.com
[3]Assistant Professor, Department of Management,
Invertis University, Bareilly, Uttar Pradesh, India, unnatiagarwal6789@gmail.com
[4]Assistant Professor, Department of Management,
Invertis University, Bareilly, Uttar Pradesh, India, divyatiwari54321@gmail.com
[5]Assistant Professor, Department of Management,
Invertis University, Bareilly, Uttar Pradesh, India, abhinavgaur30@gmail.com
[6]Professor and Head, Department of Management Studies, Adithya Institute of Technology, Tamil Nadu, India, nt_sundar@yahoo.com
ORCID: 0000-0002-1303-2947

How to cite this article: Deepesh Tiwari, Rakesh Gupta, Unnati Agarwal, Divya Tiwari, CA Abhinav Gaur, Sundarapandiyan Natarajan, (2024) Securing the Supply Chain: Leveraging IoT and Blockchain for Financial Risk Management, 44(3), 1614-1619.

Abstract:
The needs and limitations of security create impediments to the flow of supplies and distribution, both physically and logically. These "barriers," which are the result of political or perceived enhanced security needs, impair the company's ability to respond quickly and its financial and operational success. One of the key challenges for the management of supply chains is integrating the security factor into the administrative strategy, structure, and operations [1]. SCS entails taking precautions to prevent illegal goods from accessing the supply chain as well as items from exiting it. The risk to a supply chain is represented by this potential "disruption of flows between organizations" [2]. Formally speaking, supply chain risk may be defined as the distribution's volatility, value, and likelihood of supply chain outputs [3]. SCS is therefore a part of an organization's entire risk management plan. Even though supply chain risk management (SCS) is the specific subject of this study, it's crucial to place the topic of SCS within the broader framework of supply chain security management [4].

INTRODUCTION

The needs and limitations of security create impediments to the flow of supplies and distribution, both physically and logically. These "barriers," which are the result of political or perceived enhanced security needs, impair the company's ability to respond quickly and its financial and operational success. One of the key challenges for the

management of supply chains is integrating the security factor into the administrative strategy, structure, and operations [1]. SCS entails taking precautions to prevent illegal goods from accessing the supply chain as well as items from exiting it. The risk to a supply chain is represented by this potential "disruption of flows between organizations" [2]. Formally speaking, supply chain risk may be defined as the distribution's volatility, value, and likelihood of supply chain outputs [3]. SCS is therefore a part of an organization's entire risk management plan. Even though supply chain risk management (SCS) is the specific subject of this study, it's crucial to place the topic of SCS within the broader framework of supply chain security management [4].

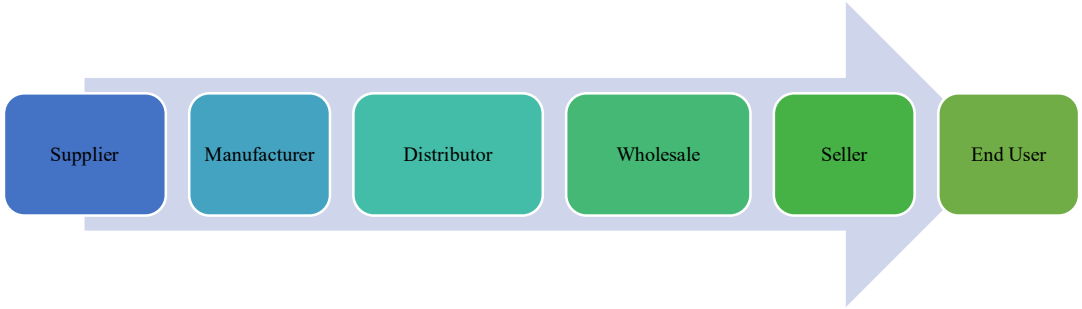

Fig. 1. Different stages of a basic supply chain [22]

As a result of the current security concerns, several projects and potential ways to improve security in global supply chains without sacrificing efficiency have been developed. Companies, authorities, and scholars are approaching the issue from many angles and with a variety of approaches. However, there are a number of academic research questions in the field of SCSM (Supply Chain Security Management) due to inherent complexities like the large number and diversity of participants involved in global supply chain processes, as well as the requirement to identify cost-effective measures for safety. Supply chain risk management is “the identification and management of risks for the supply chain, through a co-ordinated approach amongst supply chain members, to reduce vulnerability as a whole” [4]. [3] propose that supply chain management of risks is comprised of four interconnected constructs:

(1) Risk sources;
(2) Supply Chain Strategy Risk Drivers;
(3) Supply Chain Risk Management Techniques; and
(4) Supply Chain Risk Outcomes.

The conversation on supply chain security issues revolves around the idea of vulnerability. Vulnerabilities are the parts of the chain of supply that are weak and can be broken by an unfavorable occurrence. [5], [6]; vulnerability denotes the degree of damage an event would have in addition to the likelihood that an unwanted event would occur or that an attack would evade the security precautions. [5], [7] It was mentioned that the features of the transportation system lead to a number of vulnerabilities, including the logistics sector's complexity, volume, and lack of transparency; the transportation industry's interconnection; and the absence of redundancy [8].

Fig. 2. Risks in Supply Chain

Risks can disrupt operations and impact organization performance for supply chains, both externally and internally. Regulatory changes and natural disasters are some of the external risks that companies may face. Geopolitical tensions and natural disasters can also affect the international trade industry. A significant threat to internal quality control comes from operational inefficiency and quality control challenges. The supply risk arises from issues of reliability, performance, and compliance, while the demand risk comes from fluctuations and forecast errors. A cyber security threat is a malware attack or a breach in data security, whereas a currency exchange rate risk is a change in exchange rates, a delay in payment, and a credit risk is a change in the denomination of an asset. Continuity and resilience of the supply chain are essential to ensuring supply chain continuity and resilience, for this reason proactive measures are required in order to mitigate these risks and to implement robust risk mitigation strategies.

II. FINANCIAL RISK MANAGEMENT IN SUPPLY CHAIN MANAGEMENT

An intricate interaction between different entities entails different financial risks, and financial risk management is an important function aimed at identifying, assessing, and mitigating them. Due to the global nature of supply Forward contracts and currency options are used by many organizations as a way to protect against adverse changes in exchange rates.

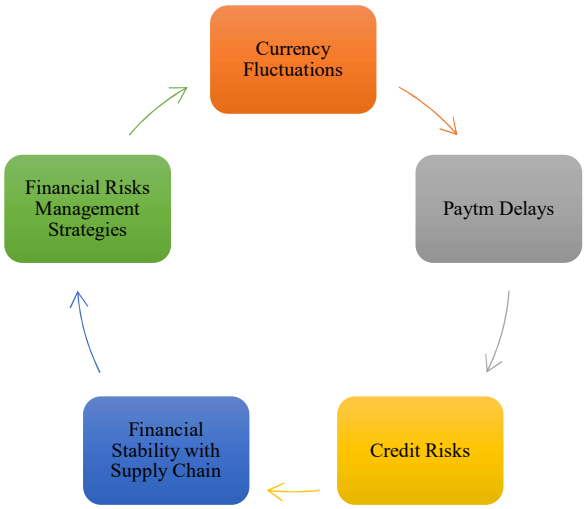

Fig. 3. Financial Risk Management in Supply Chain Management

If a customer or supplier does not pay, this can also lead to a liquidity crisis since there may be payment delays which can also disrupt cash flow and result in a cash flow crisis. It is also possible that both customer and supplier may not pay, both of which can cause a liquidity crisis. In order to alleviate these concerns, it is recommended that a payment policy be implemented and that there is clear communication with the customer in order to minimize these concerns. It's important to take into account both the credit risk and a related issue known as the loss that may occur due to defaults on the part of customers or suppliers, because they are both critical risk factors to consider. Businesses can mitigate these risks by employing strategies such as conducting a thorough credit assessment and establishing credit limits in order to mitigate these risks so that these risks can be minimized to the greatest extent possible. Additionally, it is extremely crucial that the entities that form a supply chain have an adequate financial standing so that they can continue to operate during times of uncertainty, thus ensuring that operations do not suffer. An example of the term "risk-sharing mechanism" is the process of assessing the financial health of a company's suppliers and distributors in order to share risks among them. As a proactive approach to managing financial risk in supply chains, it is imperative that we develop solid risk management policies, design contingency plans, and encourage collaboration between all parties involved in the network through the whole supply chain in order to reduce the cost of financial risk.

III. ROLE OF IoT IN SUPPLY CHAIN MANAGEMENT

Numerous scholars have examined the characteristics of supply chain robustness. The qualities of SCRes

regarding the areas of cooperation, flexibility, adaptation, visibility, and sustainability have all been covered by [9]. These characteristics lessen supply chain interruption while also facilitating competitive advantage [10].

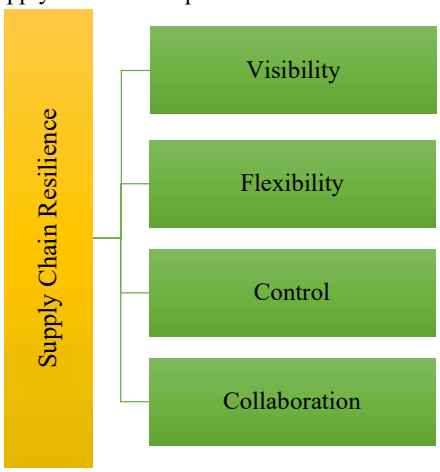

Fig. 4. Flowchart of Supply Chain Resilience [10]

The characteristics of the SCRes depicted in figure 2, which are necessary for a supply chain which can manage change and minimize interruptions, are directly impacted by the difficulties faced by traditional supply chains. Traditional supply chains faced challenges such as complexity, rising prices, errors, and elevated risks [11], [12]. Prior to IoT's introduction into the SC, information and data were only exchanged with one actor, which decreased transparency. In contrast, the smart SC allows for simultaneous cooperation with all necessary actors. Visibility was further impeded by errors, discrepancies, and data distortion through the supply chains brought about by a lack of current information and data [13].

IV.BLOCKCHAIN TECHNOLOGY FOR FINANCIAL RISK MITIGATION

Because the blockchain is a decentralised system, users may upgrade networks continuously without worrying about money. It makes information exchange easier and offers a safe network for transactions. Blockchain technology improves operational efficiency and customer experience by providing real-time recording of transactional in nature, contractual, and other information [14]. Because of its distributed ledger foundation, tamper-proof international networks are guaranteed. Due to its potential to drastically change a number of industries, most notably the financial industry, blockchain technology, namely bitcoin, has attracted a lot of attention [15]. Over a community of computers, the blockchain is a distributed, decentralized database that provides safe, transparent, and immutable transaction tracking. Fundamentally, blockchain is just a technology that makes blockchain possible. Its foundational ideas include decentralized management, cryptography security, and consensus processes [16].

V. INTEGRATION OF IoT AND BLOCKCHAIN FOR ENHANCED SUPPLY CHAIN SECURITY

While IoT operations have developed quickly thanks to the IoT-centric architecture, integrative data-driven corporate applications are not as well supported by it. Blockchain technology allows business colleagues to gather and send data without centralized coordination, improving privacy and security in IoT-based information management. But blockchain also necessitates HACCP procedures and transaction data maintenance. BC provides reasons for irreversibility and traceability, enhancing confidence in real-time and immutable information. Businesses are eager to create system for SC audits that are based on BC [17]. Creating algorithms and systems that can carry out tasks without requiring human input is essential in a digital environment [18], [19]. These apps, sometimes referred to as smart agreements, are incorporated into blockchain systems. Every blockchain node acts as a decentralised virtual machine (VM) by automatically carrying out a smart contract. But the overall system is still impacted [20].

VI. CHALLENGES AND CONSIDERATIONS IN IMPLEMENTING IoT AND BLOCKCHAIN FOR FINANCIAL RISK MANAGEMENT

There are a number of challenges and considerations involved in implementing Internet of Things (IoT) and blockchain technology for the purpose of managing financial risk in supply chains. When it comes to integrating IOT devices with existing infrastructure, integration can be a difficult and complicated task. A significant amount of capital investment is required to integrate them into the existing systems in a way that will require significant investments in hardware, software, and connections in order to get them working. In order to prevent sensitive financial information from being exposed via IoT data streams, that data streams must be secured and protected; a breach of either of these can have serious consequences. Moreover, IoT devices generate so much data that traditional risk management systems are overwhelmed, requiring robust data analytics capabilities to make effective use of it. Scalability, interoperability, and regulatory compliance play an almost similar role in the implementation of blockchain technology. Transparency and integrity must be observed over a number of parties, and a large number of transactions should be dealt with securely over the blockchain networks. It may also be difficult to navigate legal frameworks and regulatory bodies encasing blockchain implementation, which requires collaboration from all stakeholders. Overall, the challenges and concerns presented above, if addressed, will go a long way in realizing the full benefits of IoT and blockchain technology.

VII. FUTURE TRENDS AND OPPORTUNITY IN SECURING THE SUPPLY CHAIN WITH IoT AND BLOCKCHAIN

With the ability to enhance transparency, traceability, and security across supply chain operations, the two most promising technologies for supply chain security in the future are those of IoT and blockchain. IoT devices can be used in the tracking of goods, assets, and environmental conditions throughout the supply chain network in real time with the utmost affordability. In this regard, risk management will be done through proactive ways; predictive maintenance will be achieved, and logistics operations generally will be optimized. Blockchain technology, in turn, provides tamper-proof, decentralized, and immutable ledger systems that transparently record supply chain transactions and events. This enhances trust and accountability among supply chain stakeholders and greatly reduces the risk of fraud, counterfeiting, and unauthorized access to sensitive information. Smart contracting can also be created via IoT and blockchain to make the processes involved in transactions, payments, and compliance management efficient. In general, IoT and blockchain technologies for supply chain security portend a bright future in driving efficiency, resilience, and sustainability across global supply chain networks.

VIII. CONCLUSION

Hence, organizations would have to make security management in the supply chain a part of a broader context of supply chain risk management. It lays down a whole array of supply chain risks, ranging from external factors such as changes in regulatory bodies to inefficiency in operations as internal factors. Financial risk management becomes essential to reduce the risks in terms of currency fluctuation and delay in payment. The integration of IoT and blockchain technologies promises huge potential in terms of supply chain security. Although some problems exist in these technologies, dealing with them might unlock immense benefits in the form of transparency, traceability, and efficiency. All said, the future of securing the supply chain lies in harnessing the potential of IoT and blockchain technologies toward resilient and sustainable supply chain networks.

REFERENCES

[1] Hintsa, Juha, Ximena Gutierrez, Philip Wieser, and Ari-Pekka Hameri. "Supply chain security management: an overview." International Journal of Logistics Systems and Management vol 5, no. 3-4, pp.344-355, 2009.

[2] Ju¨ttner, U. “Supply chain risk management: unerstanding the business, requirements from a practitioner perspective”, International Journal of Logistics Management, Vol. 16 No. 1, pp. 120-4, 2005.

[3] Ju¨ttner, U., Peck, H. and Christopher, M., “Supply chain risk management: outlining an agenda for future research”, International Journal of Logistics: Research and Applications, Vol. 6 No. 4, pp. 197-210 ,2003.

[4] Williams, Zachary, Jason E. Lueg, and Stephen A. LeMay. "Supply chain security: an overview and research agenda." The International Journal of Logistics Management Vol.19, no. 2, pp. 254-281, 2008 .DOI 10.1108/09574090810895988.

[5] Barnes P, Oloruntoba R Assurance of security in maritime supply chains: conceptual issues of vulnerability and crisis management. J Int Managevol.11 no. 4, pp. 519–540, 2005.

[6] Wagner SM, Bode C An empirical investigation into supply chain vulnerability. J Purch Supply Manage vol. 12 no. 6 pp, 301–312. 2006

[7] Transportation Research Board Deterrence, protection, and preparation: the new transportation security imperative (No. 0309077109 (pbk.)). Transportation Research Board, Washington2002.

[8] Gould, Julie E., Cathy Macharis, and Hans-Dietrich Haasis. "Emergence of security in supply chain management literature." Journal of Transportation Security vol. 3 pp, 287-302, 2010. DOI 10.1007/s12198-010-0054-z

[9] U. Soni and V. Jain, "Minimizing the vulnerabilities of supply chain: A new framework for enhancing the resilience," in IEEE International Conference on Industrial Engineering and Engineering Management, 2011, pp. 933–939.

[10] Al-Talib, Moayad, Wasen Y. Melhem, Anthony I. Anosike, Jose Arturo Garza Reyes, and Simon Peter Nadeem. "Achieving resilience in the supply chain by applying IoT technology." Procedia Cirp vol, 91 pp, 752-757,2020.

[11] M. Abdel-basset, G. Manogaran, and M. Mohamed, "Internet of Things (IoT) and its impact on supply chain : A framework for building smart , secure and efficient systems," Futur. Gener. Comput. Syst., vol. 86 , pp. 614–628, 2018.

[12] M. A. Adeseun, A. I. Anosike, J. A. Garza Reyes, and M. Al-Talib, "Supply Chain Risk Perception: Understanding the Gap Between Theory and Practice," IFAC-PapersOnLine, vol. 51, no. 11, pp. 1701–1706, 2018.

[13] N.-O. Hohenstein, E. Feisel, E. Hartmann, and L. Giunipero, "Research on the phenomenon of supply chain resilience: A systematic review and paths for further investigation," International Journal of Physical Distribution & Logistics Management, vol. 45, no. 1/2. pp. 90–117, 2015.

[14] Javaid, Mohd, Abid Haleem, Ravi Pratap Singh, Rajiv Suman, and Shahbaz Khan. "A review of Blockchain Technology applications for financial services." BenchCouncil Transactions on Benchmarks, Standards and Evaluations vol. 2, no,3 : 100073,2022.https://doi.org/10.1016/j.tbench.2022.100073

[15] Yerram, Sridhar Reddy, Dileep Reddy Goda, RavikiranMahadasa, Suman Reddy Mallipeddi, Aleena Varghese, J. R. P. K. Ande, PavaniSurarapu, and SreekanthDekkati. "The role of blockchain technology in enhancing financial security amidst digital transformation." Asian Bus. Rev vol, 11, no. 3 , pp , 125-134, 2021.https://doi.org/10.18034/abr.v11i3.694

[16] Mahadasa, R., Goda, D. R., &Surarapu, P. Innovations in Energy Harvesting Technologies for Wireless Sensor Networks: Towards Self-Powered Systems. Asia Pacific Journal of Energy and Environment, vol,6 no. 2, pp, 101-112 ,2019.https://doi.org/10.18034/apjee.v6i2.727

[17] Jayashri, N., Veeresh Rampur, DurgaprasadGangodkar, M. Abirami, C. Balarengadurai, and Anil Kumar. "Improved block chain system for high secured IoT integrated supply chain." Measurement: Sensors vol, 25 100633,2023.https://doi.org/10.1016/j.measen.2022.100633

[18] M. Crosby, P. Pattanayak, S. Verma, and V. Kalyanaraman, ''Blockchain technology: Beyond bitcoin,'' Appl. Innov., vol. 2, no. 6–10, pp. 71, 2016.

[19]] Q. Tang and L. M. Tang, ''Toward a distributed carbon ledger for carbon emissions trading and accounting for corporate carbon management,'' J. Emerg. Technol. Accounting, vol. 16, no. 1, pp. 37–46, Mar. 2019.

[20] Learn About Ethereum, Ethereum, 2020. [Online]. Available: https://ethereum.org/en/about/

[21] Al Sadawi, Alia, Mohamed S. Hassan, and MalickNdiaye. "A survey on the integration of blockchain with IoT to enhance performance and eliminate challenges." IEEE Accessvol, 9 pp, 54478-54497,2021.10.1109/ACCESS.2021.3070555

[22] Islam, Md Didarul, Haoting Shen, and ShahriarBadsha. "Integrating blockchain into supply chain safeguarded by PUF-enabled RFID." Internet of Things vol, 18 pp, 100505,2022.