Blockchain for Challenges of Logistics and Supply Chain Information System

Devarsh S. Patel
Department of Information Technology
MPSTME, NMIMS University
Mumbai, India
devarshpatel2605@gmail.com

***Abstract*—The globalization of Logistics and Supply Chain has escalated the demand for efficiency in its Information Systems and Security. With supply chain systems now crossing the boundaries, it has become increasingly important to manage the vast amount of data it generates. Conventional supply chain system has a lot of manual tasks to be done which is time consuming and makes it prone to more errors. Supply chain systems may leverage blockchain technology (BT) to streamline supply chain operations in a trustworthy and secure way. The integration of the blockchain into supply chain systems looks promising but has a lot of challenges right now. The challenges are primarily because of the relatively new technology with lack of standards and guidelines, risk of adoption, and other risks like cost, time and information sharing. This paper investigates the challenges of logistics and supply chain and its solutions using BT followed by analysis of their pros and cons.**

Keywords— Logistics and Supply Chain Management, Challenges, Information System, Blockchain, Smart Contract.

I. Introduction

Logistics and Supply Chain Management (LSCM) is the process of procuring resources, planning, and controlling their usage, production and distribution of a product to the end users. Earlier retailers had a secondary role wherein the products were pushed on them irrespective of the customer choice or demand. But now, retailers play a crucial role at every stage and forecast the demand. This has demanded transformation of technology and information systems for supply chain significantly. Information sharing especially has been facilitated drastically [1]. LSCM Information Systems is the management of this vast data generated by the processes at every stage. Information Systems in LSCM is very essential to improve control of production, to handle the inventory efficiently, to enhance collaboration and establish trust between the parties involved, and to track and deliver orders more efficiently and securely [2]. COVID-19 caused a huge increase in demand for online purchases in turn putting a lot of pressure on LSCM. This made us realize that we need a robust and efficient LSCM which requires a strong Information System with Security to support it. BT can support the needs of LSCM and can help overcome a lot of existing problems and can also make the processes simpler and more secure.

A lot of issues can be resolved by using BT since it maintains confidentiality, integrity, and availability of all the transactions and data. LSCM Information Systems must provide the end-users, and everyone involved with accurate information at every stage of the product's life cycle. This requires information sharing which mandates establishing trust. All parties should validate the transactions done at all the stages by different parties. All parties involved are miners on a blockchain-based supply chain system. These miners broadcast a new transaction on the network when a product's status is updated or when consensus is required. Here, chances of fraud or mistake decreases since all the parties participate in the process of decision making.

In article [3], Deloitte recommends leveraging the BT to record information efficiently to manage supply chain more effectively. Seven large US corporations are now working on how can blockchain improve supply chain information system. Early studies show that it enables faster and cheaper product delivery, enables traceability, streamlines financial process flows, and improves coordination among the parties [4].

A. Logistics And Supply Chain Management

Supply chain is a series of processes that aims to meet the needs of end consumer. It is defined as "The integrated planning, coordination, and control of business processes and activities in the supply chain to deliver superior consumer value at less cost to the supply chain as a whole whilst still satisfying requirements of other stakeholders in the supply chain" by Van Der Vorst. A robust LSCM can boost profits by lowering expenses and offering improved delivery and product quality. This can be done by better information availability and collaboration [5]. LSCM is crucial for the success of a business [6]. This largescale data sharing in LSCM, makes it a necessity to have a transparent, reliable, robust, and secure system in place. Though the main stages of LSCM are known as Supplier, Manufacturer, Distributer, Retailer and Customer. *Figure 1* represents the stages of LSCM and the process at every stage.

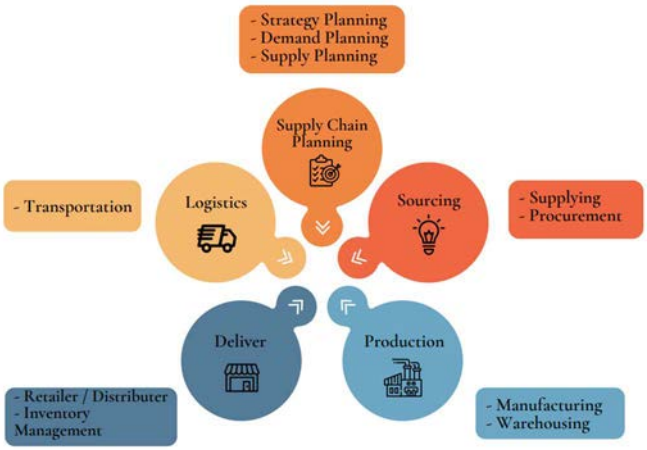

Fig. 1. Stages and processes of Supply Chain

978-1-6654-9291-1/22/$31.00 ©2022 IEEE

Generated information is passed on from one stage to another. Suppliers, Manufacturers, Distributors, Retailers, Auditors, and Consumers come together to make a vast complex network of supply chain [7]. The flow of information and process workflows needs to be streamlined to make LSCM Information Systems more efficient and synchronized. In a conventional LSCM system, the transactions are between the two parties involved at a stage, not everyone in the process comes to know about every transaction that takes place. The person that presently has the product enters its status and information. For instance, it may be necessary to split an order into many shipments or to merge several orders into one shipment, which makes it challenging to keep the orders, shipments, and payments in sync. There is a lot of scope for error at every stage of information flow and it is practically impossible to trace back the transactions to find the error. This can be resolved by the means of common consensus at every stage for all the transactions by all the parties [4].

The complexity of LSCM comes with its own set of challenges which are categorized in two stages: Planning Stage and Coordination Stage. Planning Stage challenges include data analytics for forecasting the demand, supply, and inventory management. Coordination stage challenges comprises of information sharing, transparency, traceability, building trust, and increasing communication [6].

B. Blockchain and Smart Contracts

BT has peers connected on a network who share an open and distributed ledger that records all the transactions using cryptography. It is a group of blocks that records the transaction data like information, timestamp, hash value of preceding block in the order in which they were added, and they are linked to each other cryptographically. *Figure 2* represents the blocks:

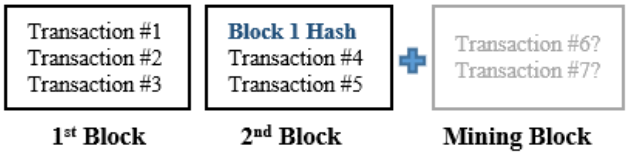

Fig. 2. Blocks in a Blockchain.

Mining must be done to add a new block to the network which is usually done by proof-of-work (PoW). Once a record has been added on the network, consensus of all the parties or a set majority is required to change the previously added blocks, increasing the security and reliability [8].

Smart contracts are immutable digital contracts that are executed across several nodes on the blockchain to ensure the consensus of the result of the contract [9]. When certain criteria or predefined conditions are met or events occur in a particular order, the smart contract is triggered, and it regulates the automatic transfer of digital assets. When a transaction is received by a miner, they are mined into the block and once this block is received by every miner on the network, the contract is then executed by all the miners [10].

There are a lot of Information System and Security challenges in LSCM that can be solved by the means of using BT. We will discuss about the challenges in Section II. In Section III we will see solutions using BT. Finally, in Section IV we will have the analysis followed by conclusion and future work in Section V.

II. Challenges & Issues In LSCM

Since there is involvement of several parties in LSCM, its information system is complicated and faces some challenges. The problems become worse as the supply chain becomes more complicated [11]. The main issues that faced by LSCM are:

1) Trust and Reputation

A major issue faced by LSCM is establishing trust and reputation among all the involved parties [12]. Parties fear sharing their private information for various business and strategic purpose. Traditional LSCM works on a stage-to-stage basis wherein not all the parties have the access to necessary information, updates and changes leading to lack of co-ordination. Lack of Inventory sharing caused by lack of trust makes the vendors keep large inventories which leads to dead stock. Better trust is very essential for enhanced information collaboration among all the parties.

2) Counterfieting

Counterfeiting is piracy i.e., making a facsimile product and selling it. Fraudulently manufactured or mislabeled products appear to the customers as if they are legitimate. Counterfeiting directly impacts sales and profits. It has adverse effects on public safety and health [11]. Due to lack of traceability, products can be tampered, or forged products can be pushed in. Smart contracts enable asset tracking, transparency and better licensing of products and services. A 2010-2012 US study revealed that 87% of the time the seafood is mislabeled. More than 2% of the world's economic output, according to PwC, is attributable to earnings from counterfeiting. Online counterfeiting caused 323 billion USD in damages in 2017, according to the Global Brand Counterfeiting Report 2018. In terms of lost revenue from prescription of drugs alone, counterfeit consumer goods are responsible for around 188 billion. Also, Blockchain makes it possible for a person to confirm how ethically and accurately a thing was acquired [7]. Strict monitoring and disciplinary actions must be in place to tackle this issue.

3) Demand Forecasting

Whenever it comes to demand forecasting, the greatly increased data quality translates to an equally considerable value for the business [13]. Since it is challenging to get data that can be trusted, demand forecasting is a complex task for the supply chain management of many businesses. The predictions of consumer products and services were effectively broken by COVID-19, leaving companies without a direction as to how much stock to hold or produce at any moment [13]. Lack of reliable data and its real-time visibility causes demand forecasting difficult.

4) Third Party Information Access

Many in the supply chain depend on third parties for some of their processes. These third-party vendors possess security risk because they have access to the private data and information. These vendors do not have cyber protection

which leads to data breaches [11]. Another issue is third party regulator for quality control check. Quality check should be performed correctly at all the stages. Also, the location of third parties become a problem to facilitate transactions. For instance, an agent based in the United States cannot set up the escrow when one of the parties involved in the transaction is in North Korea. [14].

5) Payment Discrepancies

Manual invoicing is prone to a lot of errors and is tasking since it requires manual documentation. It is very inefficient in terms of cost and time [11]. There are many payments related discrepancies in the current supply chain like late payments, conditional payments, and unfulfilled commitments. Third party's involvement in agreements and payments also leaves a big scope for error and fraud.

6) Physical Documentation

Physical documentation sharing leads to inefficient co-ordination among the involved parties [11]. This causes a decreased visibility of the product. Lack of data sharing platforms makes it difficult for all the parties to co-ordinate and share information [15].

7) Cyberattacks

Cyberattacks are very frequent because the LSCM is a very big and complex process. Having so many stages and parties involved, there are multiple areas of vulnerability. The attacker will go for the weakest one [11]. It is also very difficult to predict the risk and vulnerabilities [16]. Intellectual Property and Sensitive data should be protected. The primary risk aspect in supply chain cyberattacks is the likelihood of illegal alterations occurring and its severity [17].

III. BLOCKCHAIN BASED SOLUTIONS

Blockchain has the potential to resolve some of the issues with its properties and applications. They are discussed below:

1) *Distributed Ledger for Provenance Tracking [Solution to Section II (1), (2), (3), (6), (7)]*

Strict monitoring and verification should take place at every stage [18]. Provenance Tracking using smart contracts enables the stakeholders to track the origin, changes, and record of the product [11] [6]. By offering transparency, provenance leverages blockchain to increase supply chain trust [5]. Human error, additional costs, and time delays related to transactions in a conventional LSCM can be reduced by using blockchain-enabled provenance tracking. Every new article should be assigned a digital token indicating the origin. This token should be passed along with the physical article. This token is a virtual certificate of authenticity. Walmart used the blockchain-based ecosystem in China which improved confidence, allowing supply chain parties to submit certificates of validity to the blockchain [11]. Smart contracts make sure that the agreements are upheld automatically eliminating the fear of not holding up to the agreed contract. This establishes trust. Using BT makes it difficult to tamper with products, to push in forged products and to steal products since all the original products are traceable and decisions requires consensus by all the parties. If a product is missing or is tampered, then we can know the stage at which it occurred. In [19], P. Saindane, Y. Jethani, P. Mahtani, C. Rohra and P. Lund proposed a system for traceability, security, and transparency using blockchain and IoT to solve the issue of counterfeit. RFID's can be used for supply chain tracking since they provide real time location of the product which can help in overcoming thefts and counterfeit and the customer feels more secure and gains confidence. Distributed ledger of blockchain can enable a decentralized inventory sharing providing real time access about the inventory for the information of the products which helps all the parties to be updated and establishes a secure environment with trust. It enhances the speed, traceability, transparency, and visibility while eliminating the need to maintain physical documents [11]. It also makes the information maintenance easier and reduces the delays caused due to paperwork [11]. The data collected on sales, inventories, manufacturing, and other areas are critical to the precision of demand forecasting efforts; but, businesses are concerned about the hazards associated with providing more information than they should [13]. Integrating blockchain technology, on the other hand, does not always imply relinquishing ownership of all of the data or the traditional systems that store it [13]. They are able to exchange information on a permissioned basis in a more secure manner inside a blockchain network without losing control over it, and they are even able to trace the usage of the data in order to properly manage remuneration for the use of the data [13]. Blockchain could complement with techniques like CERT Resilience-Management Model (CERT-RMM), the External Dependencies Management (EDA) methodology, and the Security Engineering Risk Analysis (SERA) framework to give the whole software supply chain a more secure provenance [17]. Digital signatures should be used for authorizations.

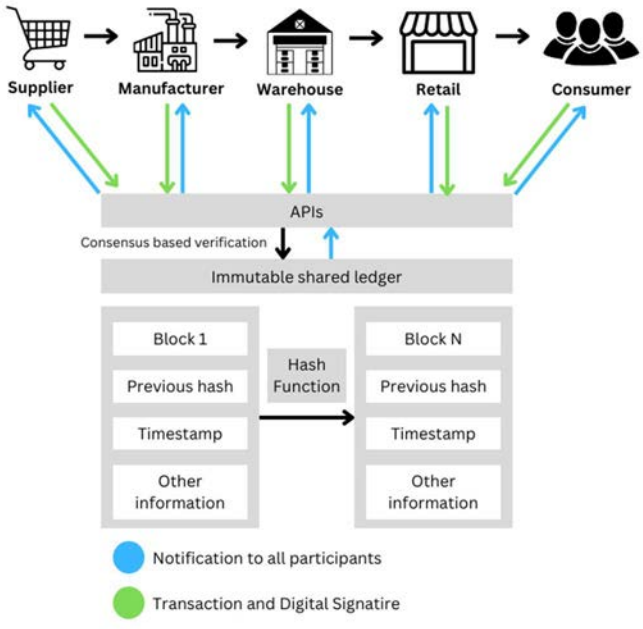

Fig. 3. Framework for Provenance Tracking

2) *Third Party Vendors on Blockchain [Solution to Section II (4)]*

Vendors should be made a part of the blockchain so that the information stays within the blockchain. This ensures security of information while taking help from the third parties. A. K. Goharshady, in [20] claims that The Dapp community is incorrect in its assumption that the two-party escrow solutions now in use have a clever mechanism that encourages rational actors to tell the truth and discusses how it is necessary to rely on third parties (escrow agents) for smart contracts and transactions.

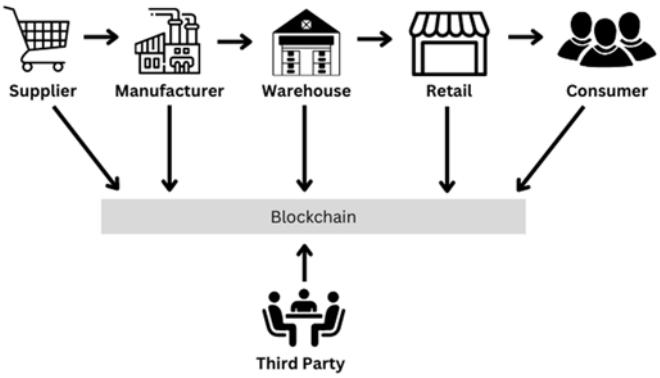

Fig. 4. Third party on blockchain

3) *Smart Contracts for Automation and Payment [Solution to Section II (1), (5)]*

Smart contracts enable automatic payments which is a safe option between untrusted parties. Smart contracts can digitalize and automate the invoicing and contractual agreements [11]. They make sure that the agreement is fulfilled. When certain predefined conditions are met or when an event like “trade has been completed” is triggered, the payment can then be made automatically. If the payment must be done before the delivery, then the smart contract can be designed to hold the delivery until the payment is received [6]. Law, Angwei proposed smart contract-based methodology that all the parties will have access to. Three Solidity smart contracts are used as a proof-of-concept to manage the chain of custody as items move through a supply chain, identify the origin of commodities, execute payments automatically when requirements are met, and keep an open database of stakeholders with a reputation score [6].

S. Wang et al proposes an idea of a blockchain-based system for product traceability, wherein product transfer histories are constantly being recorded in an immutable ledger. This entire method of product registration, transfer, and tracking is made possible by the cooperation of smart contracts [21].

I. A. Omar et al. recommend a procedure for exchanging inventory that is built on a private Ethereum smart contract using blockchain to link suppliers and retailers. To increase trust and securely communicate information, algorithms are suggested [1]. M. Mylrea and S. N. G. Gourisetti proposed a blockchain based solution using smart contract for security of energy supply chain. Dynamic patch management notifications and updates, role-based constraints, baselining and monitoring machine state integrity, and other procedures may all be used to automate supply chain security.

Smart contracts are given a particular address. Using that address, you may communicate with the smart contract. This particular smart contract may be found on the blockchain in the form of bytecode. Blockchain offers a unique way of distributing trust by providing a cryptographic signed distributed ledger that can be atomically confirmed. Critical supply chain information is maintained in the distributed escrow of the blockchain, which keeps time-stamped data blocks that cannot be modified retroactively, increasing the reliability and probity of the data, as opposed to supply chain data like inventory of critical hardware or time, date of patch for critical software. [9].

S. Su, K. Wang and H. S. Kim, in SmartSupply, developed an effective smart contract in order to arrange the miners' local data structure in order to facilitate transaction verification and information extraction. They carried out one million transactions over the course of three hours and found that 30% of the miners were malicious, resulting in an average response time of 0.0723 seconds. One million transactions results into the blockchain increasing to 500 million bytes in size. Their solution ensures consistent time latency per query regardless of the length of the blockchain, resulting in a significant reduction in the amount of time needed to respond to query requests when compared to the conventional architecture. [10].

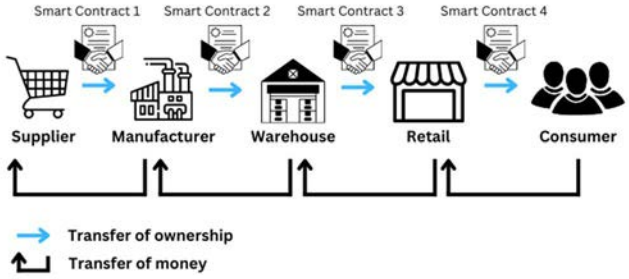

Fig. 5. Smart Contract for Payment

IV. ANALYSIS

Table 1 discusses the pros and cons of the solutions and properties of the blockchain technology.

V. CONLUSION & FUTURE WORK

This paper presented a systematic study on how Logistics and Supply Chain Information Systems work and how blockchain can be leveraged to make LSCM Information Systems and Security more efficient and secure.

To conclude, implementing blockchain requires high computational power and resources. On the contrary, if cheaper methods are used then some of the benefits of blockchain are lost. Even after consuming such high computational power, the throughput is low meaning lesser LSCM transactions per second as compared to a centralized system. Organizations are also preferring sustainability over a long-term attempt to use a new technology. For LSCM, blockchain needs to be integrated with other technologies like IoT, Cybersecurity, RFID and many more [5]. Poor integration will cause a lot of functional problems. The cost

Table 1. Pros and Cons of the solutions

Sr No	Solution / Method by Blockchain Technology (BT)	Pros	Cons
1.	Distributed Ledger for Provenance Tracking	1) Reduce human burden, error, cost and delay [11]. 2) Transparency for authorization. 3) Better visibility & traceability. 4) Limited third-party involvement. 5) Reduced Paperwork. 6) Easy maintenance of information. 7) Secured transactions. 8) Access to up-to-date inventory. 9) Assists in demand forecasting.	1) Lack of Organizational readiness. 2) Lack of technical expertise & infrastructure. 3) Lack of legal and regulatory compliance. 4) High risk and investment for technology adoption. 5) Interoperability and integration issues [8]. 6) Upwards scalability increases response time and fees. 7) Resource and energy demanding [6].
2.	Third Party Vendors on blockchain	1) Security to private information. 2) Establishes trust.	1) Vendor must get involved separately with every party on their blockchain. 2) Costly. 3) Resource demanding.
3.	Smart Contracts for Automation and Payment	4) Helps automate processes. 5) Reduces burden, error and saves time. 6) Reduces or eliminates reliance on third party for payment & agreements. 7) Cross border agreements and payments.	1) Immutable so agreement should be without errors [6]. Errors will be permanent. 2) Lack of standards & guidelines. 3) Lack of legal practices and regulations. 4) Lack of security of models. 5) Country of business is a barrier.

risk involved with implementing blockchain makes the organization reluctant to invest in the technology. The technology itself is in its initial stages. It requires a lot of work to be done before it can be fully reliable. Moreover, considering LSCM, with so many parties and processes involved, it becomes even more difficult for LSCM to implement blockchain on a very large scale. Scalability and adoption to the technology by various parties involved becomes a challenge for LSCM. All the parties need to invest time and cost in the technology on their end to make the functioning of the entire cycle secure, robust and efficient. Blockchain for LSCM has great potential but is still at a naïve stage and requires to be regulated to be widely accepted.

The following is the future scope for Blockchain in Supply Chain:

1) Advance works on permissioned blockchains.
2) Establishing standards, guidelines, regulations and legal practices.
3) Integrating blockchain with other technologies like IoT, RFID etc efficiently.
4) Enhancing scalability, security, interoperability, and integration.

REFERENCES

[1] I. A. Omar, R. Jayaraman, M. S. Debe, H. R. Hasan, K. Salah and M. Omar, "Supply Chain Inventory Sharing Using Ethereum," *IEEE Access,* vol. 10, pp. 2345-2356, 2021.

[2] "The Sole of Information Systems in SCM is Expanding," 27 April 2021. [Online]. Available: https://online.uncp.edu/articles/mba/information-systems-role-in-scm.aspx.

[3] "Using blockchain to drive supply chain transparency," [Online]. Available: https://www2.deloitte.com/us/en/pages/operations/articles/blockchain-supply-chain-innovation.html.

[4] V. Gaur and A. Gaiha, "Building a Transparent Supply Chain," June 2020. [Online]. Available: https://hbr.org/2020/05/building-a-transparent-supply-chain.

[5] M. . R. Nur , L. Hakim and . Y. Amrozi, "CHALLENGES IN USING BLOCKCHAIN FOR SUPPLY CHAIN MANAGEMENT INFORMATION SYSTEMS," *J@ti Undip: Jurnal Teknik Industri,* vol. 15, pp. 82-92, June 2020.

[6] A. Law, *Smart contracts and their application in supply chain management,* Massachusetts Institute of Technology, 2017.

[7] "Blockchain in Supply Chain Management," [Online]. Available: https://consensys.net/blockchain-use-cases/supply-chain-management/.

[8] P. Dutta, T.-M. Choi, S. Somani and R. Bhutala, "Blockchain technology in supply chain operations: Applications, challenges and research opportunities," *Transportation Research Part E: Logistics and Transportation Review,* vol. 142, October 2020.

[9] M. Mylrea and S. N. G. Gourisetti, "Blockchain for Supply Chain Cybersecurity, Optimization and Compliance," in *2018 Resilience Week (RWS)*, 2018.

[10] S. Su, K. Wang and H. S. Kim, "Smartsupply: Smart Contract Based Validation for Supply Chain Blockchain," in *IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, 2018.

[11] V. Hassija, V. Chamola, V. Gupta, S. Jain and N. Guizani, "A Survey on Supply Chain Security: Application Areas, Security Threats, and Solution Architectures," *IEEE Internet of Things Journal,* vol. 8, no. 8, pp. 6222-6246, April 2021.

[12] B. Zalud, "The Daily Challenges of Supply Chain Security," 1 April 2016. [Online]. Available: https://www.securitymagazine.com/articles/87010-the-daily-challenges-of-supply-chain-security.

[13] R. Donekal, "How Blockchain Can Solve Demand Forecasting Problems," 20 November 2019. [Online]. Available: https://chainyard.com/insights/how-blockchain-can-solve-demand-forecasting-problems/.

[14] "H.R.757 - North Korea Sanctions and Policy Enhancement Act of 2016," February 2016. [Online]. Available: https://www.congress.gov/bill/114th-congress/house-bill/757.

[15] M. Pratap, "How is Blockchain Disrupting the Supply Chain Industry?," 8 August 2018. [Online]. Available: https://hackernoon.com/how-is-blockchain-disrupting-the-supply-chain-industry-f3a1c599daef.

[16] "Cyber Security Risk in Supply Chain Management: Part 1," 12 March 2015. [Online]. Available: https://resources.infosecinstitute.com/topic/cyber-security-in-supply-chain-management-part-1/.

[17] E. Kanal, "Could Blockchain Improve the Cybersecurity of Supply Chains?," Carnegie Mellon University's Software Engineering Institute Blog, 4 November 2019. [Online]. Available: https://insights.sei.cmu.edu/blog/could-blockchain-improve-the-cybersecurity-of-supply-chains/.

[18] R. Coates, "Counterfeits Are Still A Major Problem," 11 February 2019. [Online]. Available: https://www.scmr.com/article/counterfeits_are_still_a_major_problem.

[19] P. Saindane, Y. Jethani, P. Mahtani, C. Rohra and P. Lund, "Blockchain: A Solution for Improved Traceability," in *2020 International Conference on Electrotechnical Complexes and Systems (ICOECS)*, 2020.

[20] A. K. Goharshady, "Irrationality, Extortion, or Trusted Third-parties: Why it is Impossible to Buy and Sell Physical Goods Securely on the Blockchain," in *2021 IEEE International Conference on Blockchain (Blockchain)*, 2021.

[21] S. Wang, D. Li, Y. Zhang and J. Chen, "Smart Contract-Based Product Traceability System in the Supply Chain Scenario," *IEEE Access,* vol. 7, pp. 115122-115133, 2019.