Volume 12. No. 2
April - June 2023

ISSN-2277-5110
E-ISSN-2277-5250
Subscribers copy
Not for sale

i-manager's

Journal on Information Technology

Experience Information Technology at the Speed of Life

i-manager® Publications

ISSN: 2277-5110
Volume 12. No. 2
April - June 2023

i-manager's

Journal on Information Technology

About the Journal

i-manager's Journal on Information Technology provides a forum to the academics, professionals and advanced level students in IT for exchanging significant information, productive ideas associated with information technology and future prospects in the areas of contemporary information and communications technology. Technology changes so rapidly and the Journal aims to publish high quality papers from academia and practitioners in all areas pertaining to Information Technology and disseminate Knowledge on the same.

i-manager's Journal on Information Technology is presently in its 12th Year. The first issue was launched in 2012.

i-manager's Journal on Information Technology is published by i-manager Publications, one of India's leading Academic Journal Publisher, publishing 38 Academic Journals in diverse fields of Engineering, Education, Management and Science.

Why Publish with us

i-manager Publications currently publishes academic Journals in Education, Engineering, Scientific and Management streams. All of i-manager's Journals are supported by highly qualified Editorial Board members who help in presenting high quality content issue after issue. We follow stringent Double Blind Peer Review process to maintain the high quality of our Journals. Our Journals target both Indian as well as International researchers and serve as a medium for knowledge transfer between the developed and developing countries. The Journals have a good mix of International and Indian academic contributions, with the peer-review committee set up with International Educators.

Submission Procedure

Researchers and practitioners are invited to submit an abstract (200 words)/Full paper on or before the stipulated deadline, along with a one page proposal, including Title of the paper, author name, job title, organization/institution and biographical note.

Authors of accepted proposals will be notified about the status of their proposals before the stipulated deadline. All submitted articles in full text are expected to be submitted before the stipulated deadline, along with an acknowledgment stating that it is an original contribution.

Review Procedure

All submissions will undergo an abstract review and a double blind review on the full papers. The abstracts would be reviewed initially and the acceptance and rejection of the abstracts would be notified to the corresponding authors. Once the authors submit the full papers in accordance to the suggestions in the abstract review report, the papers would be forwarded for final review. The final selection of the papers would be based on the report of the review panel members.

Format for Citing Papers

Author surname, initials (s.) (2023). Title of paper. i-manager's Journal on Information Technology, 12(2), xx-xx.

Copyright

Contact e-mails

editor@imanagerjournals.com
submissions@imanagerpublications.com

ISSN: 2277-5110
Volume 12. No. 2
April - June 2023

i-manager's

Journal on Information Technology

Abstracting / Indexing

ISSN: 2277-5110
Volume 12. No. 2
April - June 2023

i-manager's

Journal on Information Technology

OUR OFFICES

Registered Office

3/343,Hill view,
Town Railway Nager,
Nagercoil, Kanyakumari District - 629001
Ph : 91-4652- 277675
E-mail : info@imanagerpublications.com

Editorial Office

13-B, Popular Building,
Mead Street, College Road,
Nagercoil, Kanyakumari District - 629001
Ph : (91-4652) 231675, 232675, 276675
E-mail : editor@imanagerjournals.com

Join with us

https://www.facebook.com/imanInformTech/

https://www.facebook.com/imanagerPublishing/

https://twitter.com/imanagerpub

CONTENTS

EDITORIAL

The current issue of i-manager's Journal on Information Technology (JIT), (April - June 2023: Volume – 12 Issue - 2) has five peer reviewed research papers that presents various subjects associated with Information Technology.

Anthonia Eghieso Omehia et al. examines the transformative role of ResearchGate in improving collaboration among Library and Information Science (LIS) researchers. By exploring the myriad features and possibilities, this study uncovers how it has redefined the way professionals in LIS engage with one another, share their findings, and contribute to the advancement of their field. The emergence of digital platforms has revolutionized the landscape of academic collaboration, and ResearchGate stands as a beacon of opportunity for researchers in the field of LIS.

Harry Kachule et al. present an IoT-based system, to detect gas leakage and monitor safety whenever gas equipment is being used at home. It will use the Brute Force algorithm and the BCrypt algorithm as well, which is a password hashing function. In Malawi, due to the current shortage of energy and power, people have turned to other sources of energy and power, frequently using gas for cooking and other activities. Therefore, there is a high and increasing number of gas leakage threats, which are becoming a significant concern for daily lives in Malawi.

Francis Makwinja et al. address the pressing challenges faced by ESCOM (Electricity Supply Corporation of Malawi) in effectively managing and optimizing electricity distribution within their infrastructure. This paper introduces an IoT-based industrial management system designed to tackle these challenges and enhance ESCOM's operational efficiency, energy management and overall performance.

Bethapudi et al. presents a review on Blockchain-based Supply Chain Management (SCM) and provides transparency and agreement-outsourced contract manufacturing and enhancing an organization's position as the main leader in responsible manufacturing. In this study, block chain and its effects on SCM are discussed, along with security issues and solutions.

Kondapalli Beulah et al aim to detect gas leakage using a CNN-based approach. Industrial gas-detection sensors and their placement are discussed. Sensor selection and placement are crucial to obtain accurate results. The smart monitoring system of the sensor data and monitoring mechanism are discussed in this study. CNN is promising and more accurate for gas leakage detection than the existing models for gas leakage detection.

We extend our profound thanks to the authors for their contribution towards this issue and we are grateful to the reviewers for spending their quality time in reviewing these papers. Our special thanks to the Editor-in-Chief Dr. Mohammed A. Abdala for his constant support and efforts in further enhancing the quality of the Journal.

Hope this issue imparts an enlightening reading experience! Enjoy Reading!

Warm regards,

Renisha Winston
Editorial Director
i-manager Publications

BLOCKCHAIN-BASED SUPPLY CHAIN MANAGEMENT (SCM)

By

BETHAPUDI RATNAKANTH * R. YADAGIRI RAO ** INDIGIBILLI SATYANARAYANA ***

*-*** Department of Computer Science and Engineering, Sri Indu Institute of Engineering and Technology, Sheriguda, Ibrahimpatnam, Hyderabad, India.

Date Received: 02/10/2023 Date Revised: 10/10/2023 Date Accepted: 28/10/2023

ABSTRACT

A blockchain is a decentralised, unchangeable ledger that makes it easier to track assets and record transactions in a corporate network. In a blockchain network, anything valuable may be recorded and traded, lowering the risk and increasing efficiency for all parties. It has the potential to drive cost-saving efficiencies and enhance the consumer experience through traceability, transparency, and tradeability. Blockchain-based Supply Chain Management (SCM) can provide services to participants to inquire about product details, cost, quantity, quality, availability of products, location and other significant information. It provides transparency and agreement-outsourced contract manufacturing and enhances an organization's position as the main leader in responsible manufacturing. In this study, blockchain and its effects on SCM are discussed, along with security issues and solutions.

Keywords: Blockchain, Security, Supply Chain Management (SCM), Decentralization, Phishing, Crypto Currencies.

INTRODUCTION

Information is essential to a business. It is best if it is received quickly and accurately. Blockchain is the best technology for delivering this information because it offers real-time, shareable, and entirely transparent data that are kept on an immutable ledger and accessible exclusively to members of a permissioned network (Sahoo et al., 2022). A blockchain network can track orders, payments, accounts, and production. Traditional database methods present a number of difficulties in storing financial transactions.

Transactions must be monitored and verified by a dependable third party to prevent legal problems. The existence of this centralized authority not only makes the transaction more difficult but also establishes a weak spot. Both parties can be harmed if the main database is compromised. Blockchain eliminates these problems by developing a decentralized, unchangeable mechanism for transaction recording (Agarwal et al., 2022). Blockchain generates separate ledgers for both the buyer and seller in the case of real estate transactions. All transactions are subject to both parties' approval and are automatically updated in real time in both ledgers. Any tampering with earlier transactions taints the entire ledger. These characteristics have made blockchain technology useful across a range of industries, including the development of virtual currencies such as Bitcoin (Biktimirov et al., 2017).

i-manager Publications
Member of:

This paper has objectives related to SDG

9 INDUSTRY, INNOVATION AND INFRASTRUCTURE

1. Key Elements of Blockchain

The key characteristics of blockchain technology are as follows.

1.1 Decentralisation

In the context of blockchain, decentralization refers to the transfer of power and responsibility from a centralized entity (an individual, an organization, or a group) to a dispersed network. Transparency in decentralized blockchain networks helps players build less trust in each other. These networks also prevent users from interfering with one another in ways that would impair the network's

performance (Blossey et al., 2019).

1.2 Immutability

Something can never be altered or changed if it is immutable. Once someone adds a transaction to the shared ledger, it cannot be changed by another participant. To correct an error in a transaction record, a new transaction must be added and both transactions are accessible to the network.

1.3 Consensus

Blockchain systems create regulations regarding participant consent for recording transactions. New transactions can only be recorded until the majority of network users have given their approval.

2. Structure of Blockchain

Blockchain is a ledger that tracks agreements or transactions between nodes or other network users (Yaga et al., 2019). In a blockchain, a block is typically formed after a transaction is submitted and accepted by all other users. Each block is composed of data, timestamps, block hash value, and hash value of the block before it. As each block records the hash value of the previous block, establishing a chain, the blocks are cryptographically connected. The hash value of the block is altered when a transaction is modified, severing the block's cryptographic connection. Figure 1 shows the structure of a blockchain (Chang et al., 2022).

2.1 Blockchain In Supply Chain Management (SCM)

Supply chain organizations can use blockchain to document production updates to a single shared ledger, providing total data visibility and a single source of truth,

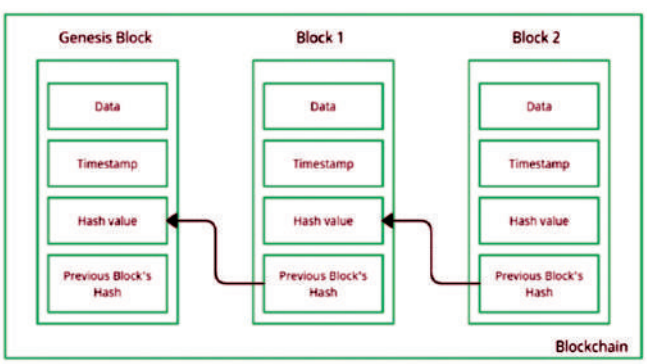

Figure 1. Blockchain Structure

and can access a product's status and location at any moment because transactions are constantly time-stamped (Dursun et al., 2022). Blockchain technology in supply chain networks enables companies to react quickly to recall. It keeps track of every action food products take before reaching the grocery shelves. Consequently, businesses can find defective products within seconds. The immutable and transparent record of all supply chain transactions is a hallmark of blockchain. This makes it easier to track things from their point of origin to their final destination, enhances accountability, and lowers the possibility of fraud. It is used in many industries, such as food and agriculture, pharmaceuticals, manufacturers, and mining (Chang et al., 2019).

Blockchain enables businesses to comprehend their supply chains and interact with customers using authentic, verifiable, and unchangeable data (Saberi et al., 2019). By gathering important data points, such as certificates and claims, and then making this information freely accessible to the public, transparency helps foster confidence. Figures 2 and 3 shows the traditional supply chains and supply chains with supply blockchain.

3. Importance of Blockchain Technology for Supply Chains

3.1 Increasing Supply Chain Complexity

In the past, supply chains were linear and had a limited number of partners. The supply chains of today are highly complicated and frequently not chronological. With several suppliers, manufacturers, logistical partners, storage partners, and other parties involved, modern supply chains are multi-tiered networks. It is challenging to carry out actions that are visible and efficient when the system grows extremely complex. Blockchain technology provides the inherent transparency, distribution, and immutability that supply networks require (Gurtu & Johny, 2019). Figure 4 represents the blockchain-based product management.

3.2 Increased Illegal Activities and Fake Goods

Assuring the legality of raw materials and components is one of the main issues faced by supply chains (Lyasnikov et al., 2020). It is difficult to track each step in a supply

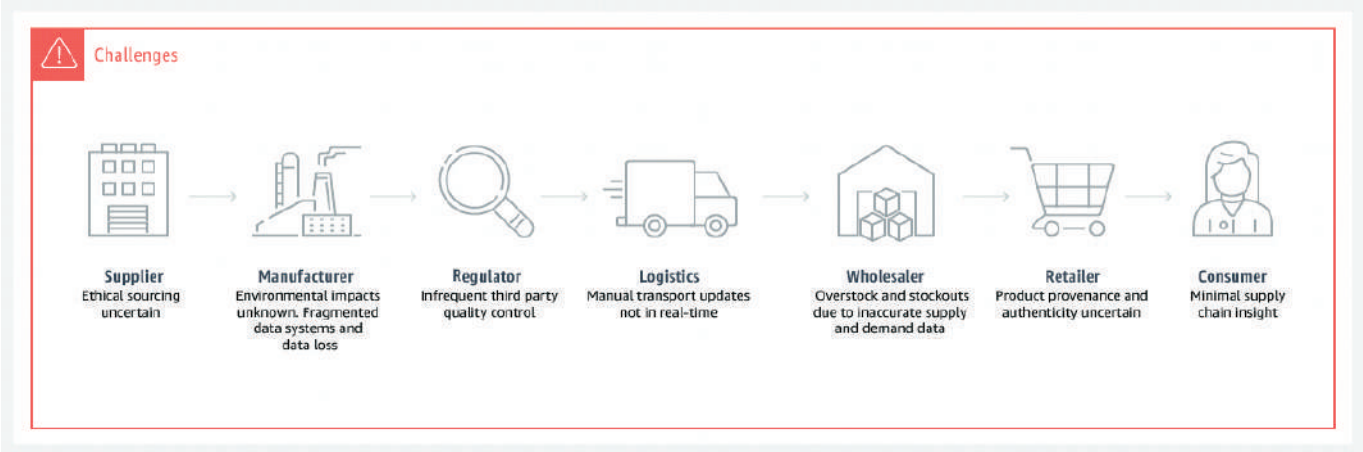

Figure 2. Traditional Supply Chains

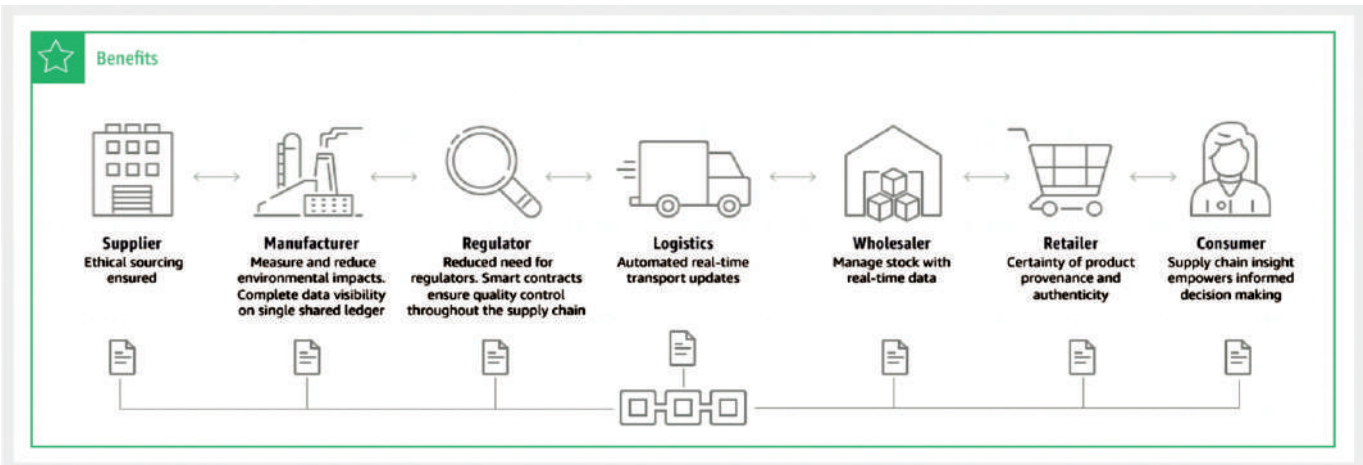

Figure 3. Supply Chains with Blockchain

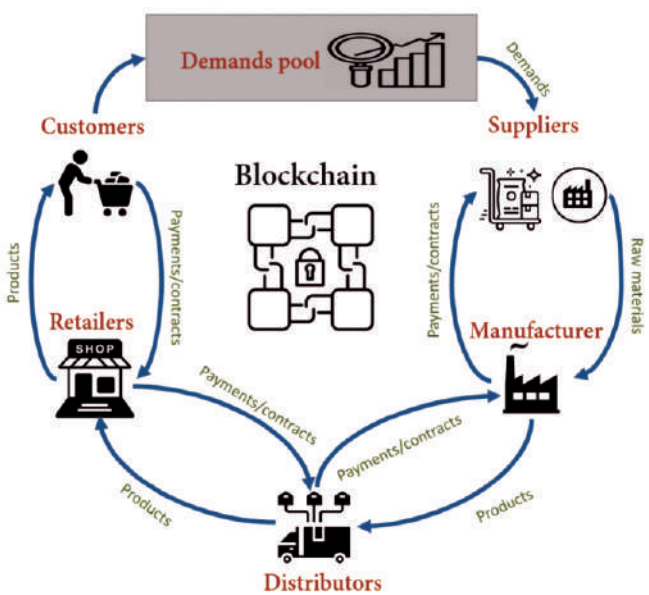

Figure 4. Blockchain-Based Product Management

chain when it spans numerous locations and has hundreds of partners. For example, it can be challenging to determine whether a supplier obtains raw materials through unethical practices. Another problem is determining whether things are genuine or fake. Fake goods may infiltrate the supply chain if there is no system in place to track each product back to its source. Therefore, supply chains require technology that enables networks to track every product back to its source. The traceability of the blockchain ledger technology is a key characteristic (Sahoo et al., 2022).

4. Security Issues in Blockchain for Supply Chain Management

The transfer of goods and services from one location to another is important in supply chain management. The

procedure entails several exchanges between numerous stakeholders, including producers, suppliers, distributors, and clients (Chang et al., 2022). These transactions generate a significant amount of data, which must be handled, tracked, and documented. Due to its intrinsic characteristics such as immutability, transparency, and decentralization, blockchain technology offers a perfect option for controlling supply chain activities. However, the effectiveness of supply chain management depends on the security of the blockchain networks (Hasan et al., 2022).

4.1 51% Attack

When one company or group controls more than 50% of the computer power on a blockchain network, this is called a 51% attack. Therefore, they can manipulate the network, change transactions, and participate in double spending.

One of the important concepts is that computing power is crucial for obtaining majority control over the hash rate of a blockchain using malicious entities. The result of a 51% attack is that a compromised blockchain can result in the reversal of transactions and the possibility of double spending. In 2018, some of the popular cryptocurrency platforms faced issues regarding 51% attacks. These platforms are Ethereum classic, Zencash, and Verge (Bhushan et al., 2022). In addition, enterprises almost lost $20 million dollars per annul due to a 51% attack. To avoid this attack on the blockchain, SCM must take some careful measures. These are continuous monitoring of mining pools, taking care of the fast hash rate, and not participating in the use of proof-of-work consensus mechanisms.

4.2 Phishing and Malware Attacks

Blockchain is no exception to the prevalence of malware and phishing scams in the digital world. These assaults may lead to the loss of private keys, which are required to access blockchain wallets (Kakarlapudi & Mahmoud, 2021). Users should be cautious when using connections or communications that seem suspicious and take care to protect their private keys. One of the most promising techniques is a phishing attack used by hackers. This technique was formally an attempt to obtain user credentials. In this technique, hackers send emails to wallet key owners by pretending to be an authentic authority source. Such types of emails request information regarding user credentials through fake hyperlinks. When hackers can access the credentials and sensitive information of a user, the users as well as the blockchain network are open to subsequent attacks. The growing number of phishing attacks on blockchain networks has created profound levels of concern in recent times.

The first blockchain hack online was in June 2011; in this attack, the cyber criminal was able to hold the auditor's credentials and then access the system unauthorisely. Then, the attacker was able to change the value of 1 BTC to 1 cent. The second blockchain hack occurred in March 2014. In this attack, he made use of bugs in the code, edited the transaction, and performed double spending. In this attack, the attacker changes the sender's signature and transaction ID before storing it in the ledger. By using the transaction ID, overwriting the transaction details is possible and can block the receiver, so that he cannot receive the funds further and only the attacker can.

In 2012, the overall loss of Bitcoin was $430,000 by hacking the user wallet and decrypting it from the linode's server. Bitcoin started using Bitgo's multi-signature wallet just a year before the attack. However, the wallet has certain challenges and vulnerabilities. The above issues lead to the hacker being able to attack and stole the BTC. Immediately after this attack, the company issued BFY tokens to compensate its customers (Uddin et al., 2023).

4.3 NiceHash Attack

A federal indictment was put on three North Korean computer programmers who participated in a wide-ranging criminal conspiracy to conduct a series of destructive cyberattacks, to steal and extort more than $1.3 billion of money and cryptocurrency from financial institutions and companies, one of which was NiceHash, in 2017, where $75 million was stolen (NiceHash, 2021). Another blockchain attack is the Slovenian exchange platform, where NiceHash was attacked. Immediately after this attack, Facebook announced that almost $80

million was hacked. The company evaluated the reason for these issues and how to prevent them from future days; as a result, the company suspended all transactions for a period of 24 hours.

4.4 Centralization & Interoperability

Blockchain is meant to be decentralized; however, in reality, most blockchains are centralized. This suggests that a small number of people or entities control the vast bulk of the network's computing power, thereby creating serious security issues. Blockchain interoperability is the ability of different blockchains to communicate and exchange data with one another. It might be difficult to monitor and verify transactions across different blockchains owing to fragmentation caused by a lack of interoperability, which poses a security concern.

4.5 Blockchain Endpoint Vulnerabilities

Another important instance of security risk in blockchain security is the vulnerability of the blockchain endpoints. One of the latest concerns in blockchain technology is security. For example, Ethereum trading or investment could result in a large amount of Ethereum being stored in a virtual savings account. The actual blocks in the blockchain are safe for hackers, and the wallet accounts are not safe. Moreover, many third-party vendors are important for blockchain transactions. A few third-party vendors include blockchain payment platforms, payment processors, and smart contracts. These third party vendors in blockchain can increase the vulnerability to hacking due to weaker security in apps and websites.

4.6 Routing Attack

One of the most important concerns for security and privacy is the blockchain in terms of routing attacks. Most applications in blockchain depend on a large volume of data transfer in real time. The main aspect of routing attacks in blockchain security is the obscurity. But the users of blockchain could not be able to identify the threats of routing attacks normally as everything appears in blockchain is normal. Routing attacks are generally used to extract confidential data or remove monetary benefits without disturbing the network users. Therefore, it is very open that routing attacks can be harmful as they are able to impose the reasonable damage before detection.

4.7 Blockchain Code Bugs

An example of a blockchain security breach is protocol source code. This occurred in 2010, when bad codes were used in the Bitcoin protocol and made it faulty. Using this attack, the hacker generated 184,467 billion coins, and the maximum delivery of Bitcoin was 21 million. However, the creators of blockchain Satoshi Nakamoto and Developer Gravin Anderson fixed the issue within a few hours.

4.8 Smart Contract Bugs

Due to weakness in the solidity language, the smart contract code can be vulnerable and attacked by an attacker. These are DAO, underflow, overflow, and re-entrance attacks.

4.9 Transaction Privacy Leakage

Another difficulty in blockchain technology security is the breach of transaction leakage. Transactions are transparent over the blockchain, so the behavior of users is traceable on the blockchain. Thus, security should be provided for transactions in the blockchain, and users must have a private key for their transactions.

4.10 Scalability

Scalability is a major issue for blockchains, especially as technology continues to advance. As more users join a network, the demand for computational power and bandwidth increases, potentially resulting in bottlenecks and network congestion. In addition, blockchain encryption techniques may be vulnerable to quantum computing, a new computing paradigm. The potential exposure of blockchain technology to hacker attacks presents a security risk.

5. Improvement of Blockchain Security for Supply Chain Management

Several steps can be taken to improve the security of blockchain networks to reduce security risks related to supply chain management on the blockchain. The following are a few possible actions.

5.1 Auditing

This process thoroughly checks blockchain protocol

codes vigorously before launching. Thus, we can easily detect bad code.

5.2 Utilization of Multifactor Authentication

Multifactor authentication adds an extra layer of security and aids in preventing unauthorized access to the blockchain network. Regular upgrades to the blockchain network's software help fix any potential security flaws.

5.3 Utilization of Smart Contract Audits

Smart contract audits assist in locating weaknesses in the smart contract code and guard against monetary loss.

5.4 Supply Chain Visibility

Supply chain visibility aids in spotting supply chain weaknesses and deters theft, fraud, and other nefarious behaviour.

5.5 Utilization of Encryption

Encryption adds a layer of protection to protect sensitive data. In the event of a security breach or other malicious action, regular backups help prevent data loss.

5.6 Blockchain Analytics

Blockchain analytics tools are used to identify any shady activity occurring within the blockchain network, and to stop fraud, theft, and other nefarious actions.

6. Benefits of Using Blockchain in Supply Chain

Figure 5 presents the benefits of blockchain.

6.1 Transparency

Every member of a blockchain can view every transaction. Transactions between two parties, such as manufacturers and retailers, may not be visible to a third party in typical supply chains. Each transaction in the supply chain is added as an immutable tamper-proof block using blockchain technology. All parties engaged in the supply chain can see each transaction. Supply chains are more open to the blockchain technology (TIBCO, n.d).

6.2 Enhanced Security

Execution errors are particularly likely in supply chain networks with hundreds of parties and thousands of transactions per day. These mistakes can involve missed shipments, inaccurate inventory data, and payment problems. The real-time detection of these execution faults is challenging in conventional supply chains. Verifying the source of this issue may require extensive investigation and document analysis. Execution mistakes may not be discovered after regular audits. A diagrammatic representation of the benefits of blockchain is represented in Figure5.

6.3 Immutability

Data cannot be changed or removed from the blockchain after it has been recorded without the network consent. Information about the supply chain cannot be altered without authorization, owing to its immutability, which guarantees data integrity.

6.4 Reduced Costs

The cost of running a supply chain can be reduced with the aid of blockchain technology. Blockchain can aid in lowering costs and boosting efficiency by automating inventory management, minimizing paperwork, and eliminating the need for intermediaries.

6.5 Enhanced Security

Blockchain transactions are tamper-proof because they are encrypted with a private key (or the user's digital signature) that initiates the transaction. Each partner in a supply chain with numerous partners has its own digital signature. The user's digital signature is used to safeguard transactions, such as purchase orders, when they first begin. The transaction is unchangeable, and the recipient party, such as a supplier, can confirm that the purchase order originated from a legitimate consumer. Counterfeiting a transaction is not possible because

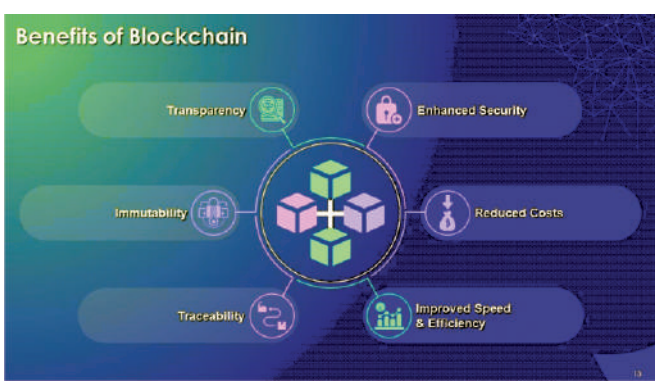

Figure 5. Benefits of Blockchain

every transaction in the supply chain is added to the blockchain as a new block. A blockchain creates a reliable sequential audit trail for all transactions that cannot be altered. Every transaction is permanently recorded using blockchain technology. A blockchain-based supply chain makes it easier and faster for firms to identify and address execution issues, thus saving time and money.

6.6 Improved Speed and Efficiency

Blockchain technology accelerates supply chain activities. Manual- or paper-based processes are digitized. Blockchain technology provides high-speed operations that are extremely responsive to changes in business conditions by streamlining real-time data flows among all supply chain players. All contracts and transactions are maintained using blockchain technology in a tamper-proof ledger. This indicates that the supply chain network contains business logic.

7. Challenges Using Blockchain in Supply Chain

7.1 Processing Large Data Sets

There is very little data on conventional blockchain applications such as cryptocurrencies. While carrying out blockchain transactions, it is simple to validate the data. Complex supply chains have large volumes of data and hundreds of transactions. Accurately streamlining this vast volume of data is crucial for integrating the blockchain into supply chains.

7.2 Blockchain Technology Standardisation

Blockchain technology vendors must standardize their offerings to be quickly adopted by numerous businesses. Some of these standards specify how two parties might concur on a block before validating it, what kind of encryption to use, or how to resolve transactional disputes.

7.3 Interoperability

Many businesses use traditional Enterprise Resource Planning (ERP) systems to handle their transactions. It could be challenging to completely replace one system before using a blockchain-based solution or to adapt these systems to use blockchain technology. It is crucial that blockchain-based solutions and legacy systems work together to some extent.

7.4 Transaction volume Management

Compared with supply chain transactions, the number of transactions per second in traditional cryptocurrency applications is quite low. High computing power is required to fully digitalize complicated supply networks. The processing speed of the blockchain network may be a constraint on how quickly transactions take place in the supply chain based on blockchain technology.

8. Applications of Blockchain in Supply Chain Networks

Transparency, traceability, and tamper-proofing are guaranteed using the blockchain technology. As blockchain technology is decentralized, it naturally satisfies the needs of supply chain networks. From financial transactions to product tracing, blockchain technology has a wide range of applications in supply chains (Rosencrance, 2023).

8.1 Finding the Source of a Product

In the majority of supply chains, raw materials come first and finished goods come last. Blockchain technology tracks a product's travel from raw material suppliers to consumers. It could be challenging for the manufacturer to establish the precise location of damaged items from many different suppliers and process them in several different factories. This problem is solved using blockchain technology, which provides traceability. With the aid of blockchain technology, the manufacturer can identify the exact shipping vessel from which the product originates. Every step in a product's journey through the supply chain results in a blockchain transaction. By ensuring product traceability, blockchain reduces product recall and revenue loss.

8.2 Making Payments using Cryptocurrency

Blockchain technology can be used to control financial flow in the supply chain, although it has not yet been widely adopted. For financial exchanges, some organizations have begun implementing blockchain-based technology such as Bitcoin. Blockchain-based money flow is transparent, simple to follow, and does not require centralized oversight.

8.3 Organising Participant Contracts

Supply chain partners can conduct smart contracts using blockchain technology. Thousands of contracts and partners are involved in complex supply chains. Each contract may be incorporated into a blockchain transaction as a block. Each of these contracts remains tamper-proof because blockchain transactions are immutable; no party can change or alter the contract.

8.4 Participant Contract Organisation

Supply chain parties can execute smart contracts using blockchain technology. In intricate supply chains, thousands of contracts and hundreds of partners exist. A blockchain transaction may contain a block that represents any of these contracts. As blockchain transactions are immutable, no party can amend or alter any of these contracts, keeping them impervious to tampering.

Conclusion

Blockchain technology is the most advanced and provides a flexible and perfect solution to the many challenges faced by conventional supply chain models. Individuals and organizations can grow and operate transparently with blockchain. Important challenges in blockchain technology include tampering actual data with malicious data, which are captured online. Blockchain technology provides an ideal solution for managing supply chain operations because of its inherent features such as immutability, transparency, and decentralization. However, the security of blockchain networks is critical to the success of supply chain management. The security risks associated with blockchain for supply chain management include malicious attacks, smart contract vulnerabilities, supply chain vulnerabilities, and insider threats. Various measures can be taken to enhance the security of blockchain networks, including the use of multi-factor authentication, regular updates, smart contract audits, supply chain visibility, encryption, regular backups, and blockchain analytics. By implementing these measures, the security of the blockchain network and the supply chain can be enhanced.

References

[1]. Agarwal, U., Rishiwal, V., Tanwar, S., Chaudhary, R., Sharma, G., Bokoro, P. N., & Sharma, R. (2022). Blockchain technology for secure supply chain management: A comprehensive review. *IEEE Access,* 85493 – 85517. https://doi.org/10.1109/ACCESS.2022.3194319

[2]. Bhushan, B., Anushka, Kumar, A., & Katiyar, L. (2022). Security magnification in supply chain management using blockchain technology. *Blockchain Technologies for Sustainability,* 47-70.

[3]. Biktimirov, M. R., Domashev, A. V., Cherkashin, P. A., & Shcherbakov, A. Y. (2017). Blockchain technology: universal structure and requirements. *Automatic Documentation and Mathematical Linguistics,* 51, 235-238.

[4]. Blossey, G., Eisenhardt, J., & Hahn, G. (2019). Blockchain technology in supply chain management: An application perspective. *Proceedings of the 52nd Hawaii International Conference on System Sciences,* 6885-6893.

[5]. Chang, A., El-Rayes, N., & Shi, J. (2022). Blockchain technology for supply chain management: A comprehensive review. *FinTech,* 1(2), 191-205.

[6]. Chang, S. E., Chen, Y. C., & Lu, M. F. (2019). Supply chain re-engineering using blockchain technology: A case of smart contract based tracking process. *Technological Forecasting and Social Change,* 144, 1-11.

[7]. Dursun, T., Birinci, F., Alptekin, B., Sertkaya, I., Hasekioglu, O., Tunaboylu, B., & Zaim, S. (2022). Blockchain technology for supply chain management. In *Industrial Engineering in the Internet-of-Things World: Selected Papers from the Virtual Global Joint Conference on Industrial Engineering and Its Application Areas, GJCIE 2020,* (pp. 203-217). Springer International Publishing.

[8]. Gurtu, A., & Johny, J. (2019). Potential of blockchain technology in supply chain management: A literature review. *International Journal of Physical Distribution & Logistics Management,* 49(9), 881-900.

[9]. Hasan, A. T., Sabah, S., Haque, R. U., Daria, A., Rasool, A., & Jiang, Q. (2022). Towards convergence of IoT and

blockchain for secure supply chain transaction. *Symmetry,* 14(1), 64.

[10]. Kakarlapudi, P. V., & Mahmoud, Q. H. (2021). Design and development of a blockchain-based system for private data management. *Electronics,* 10(24), 3131.

[11]. Lyasnikov, N. V., Smirnova, E. A., Galina, N. T., Deeva, T. V., & Vysotskaya, N. V. (2020). Blockchain technology: Supply chain management. *IIOAB Journal,* 11(S3), 1-7.

[12]. NiceHash. (2021). *North Korean hacker group indicted for 2017 NiceHash Attack.* Retrieved from https://www.nicehash.com/blog/post/north-korean-hacker-group-indicted-for-2017-nicehash-attack

[13]. Rosencrance, L. (2023). *7 Applications of Blockchain in the Supply Chain.* Retrieved from https://www.techopedia.com/7-applications-of-blockchain-in-the-supply-chain

[14]. Saberi, S., Kouhizadeh, M., Sarkis, J., & Shen, L. (2019). Blockchain technology and its relationships to sustainable supply chain management. *International Journal of Production Research,* 57(7), 2117-2135.

[15]. Sahoo, S., Kumar, S., Sivarajah, U., Lim, W. M., Westland, J. C., & Kumar, A. (2022). Blockchain for sustainable supply chain management: Trends and ways forward. *Electronic Commerce Research,* 1-56.

[16]. TIBCO. (n.d.). *The Use of Blockchain in Supply Chain for Security and Visibility.* Retrieved from https://tibco.com/reference-center/the-use-of-blockchain-in-supply-chain-for-security-and-visibility

[17]. Uddin, M., Selvarajan, S., Obaidat, M., Arfeen, S. U., Khadidos, A. O., Khadidos, A. O., & Abdelhaq, M. (2023). From Hype to Reality: Unveiling the Promises, Challenges and Opportunities of Blockchain in Supply Chain Systems. *Sustainability,* 15(16), 12193.

[18]. Yaga, D., Mell, P., Roby, N., & Scarfone, K. (2019). Blockchain technology overview. *arXiv preprint arXiv:1906.11078.* https://doi.org/10.48550/arXiv.1906.11078

ABOUT THE AUTHORS

Dr. Bethapudi Ratnakanth is currently working as a Professor and the Head of the Department of Computer Science and Engineering at Sri Indu Institute of Engineering & Technology, Hyderabad, India. He graduated with a Bachelor of Engineering (B.E) from Andhra University in 1997 and earned his Master of Engineering from Swami Ramanand Teerth Marathwada University, Nanded, Maharashtra, in 2000. In 2021, he was awarded a Ph.D. from Andhra University in the field of Blockchain Technology. With a rich experience of 22 years in teaching, research, and administration. He has established himself as an expert in the fields of Blockchain, Network Security, Image Processing, and Internet of Things. He has published over 21 papers in National and International journals and holds three patents.

Dr. R. Yadagiri Rao is currently working as a Professor and Head at Sri Indu Institute of Engineering & Technology, Hyderabad, India. He completed his M.Tech in Computer Science and Engineering from JNTUH in the year 2009. Furthermore, he obtained his Doctoral degree from Dr. B. R. Ambedkar Open University in Jubilee Hills, Hyderabad, Telangana, in February 2023. He has also published 13 papers in International journals.

Dr. Indigibilli Satyanarayana is a Principal at Sri Indu Institute of Engineering & Technology, Hyderabad, India. He received his Master's degree from the prestigious Indian Institute of Technology (IIT), Kharagpur, in 1997. In 2012, he was awarded a Ph.D from JNTUH, Hyderabad. He has an impressive publication record, with more than 70 research papers published in National and International journals, and several research papers currently under review. He boasts 21 years of teaching experience and 1.5 years of industrial experience.

3/343, Hill view, Town Railway Nager, Nagercoil
Kanyakumari Dist. Pin-629 001.
Tel: +91-4652-231675, 232675, 276675

e-mail: info@imanagerpublications.com
contact@imanagerpublications.com
www.imanagerpublications.com