Transforming Approach to Trust in the Supply Chains Through Blockchain Technology-Enabled Security.

Author[1]- Mrs. Shweta Vinay Thorat
Research Scholar- Sandip University, Nashik
Email- shweta.bhalerao93@gmail.com
Author[2]- Prof. Dr. Parimala Mani
Professor, COE, Computer Science and Application.
Sandip University, Nashik.
Email- pariguns@gmail.com

ABSTRACT

At the global level, the supply chain is becoming very hectic in various corporate sectors nowadays. The emphasis on sustainability and data security is a more crucial task to maintain digital assets. The role of digitalization in SCM very essential, it has garnered significant interest from industries, academia and government organizations and all are adopting to advanced technological features to protect confidential data. Numerous technology studies have captured various content on digital supply chain management (DSCM). Basically, the business system has changed, or SCM has adopted lots of technologies and which became DSCM. But in advance, more threats arise as problems in day-to-day life. An analysis of more techniques for protection purposes is appropriately executed, but the emerging protection systems need to be enhanced. The study examines emerging trends in Digital Signature with Blockchain Technology. Blockchain is a decentralized technology that manages all copies of the data on that system. The digital signature cryptographic technique provides end-to-end protection for secure transactions, from source to destination. The digital signature is an essential part of the legal and economic system. The number of asymmetric algorithms works in the current supply chain for advanced purposes in the public and private areas. Supply chain is widely distributed across the world as per the demand for security and has a significant impact on the government's economic ratio. This paper aims to provide strong security with authenticated digital signatures for several transactional requests.

Keywords: Blockchain, Cryptography, Supply Chain, Authentication, Hash Function, Algorithm, Keys.

I. INTRODUCTION

Today's rapidly enhanced technologies serve different ideas or techniques as well and the digitally focused world has opened the door to various advanced ones. Thus, supply chain management plays an essential role in the Indian economy for every era, including pharmaceutical medicine companies, engineering software and hardware products companies, agricultural goods, electrical appliance goods, etc. Security is an important term in that regard. In supply chain management, transactions will be transparent and have strong relationships between end users. Suppose serious attacks occur in routine; other essential functions will be affected and create barriers in communication and transactions, and those two important aspects collapse actual markets and financial mechanisms. Still, many times, issues about protecting the confidentiality, integrity, and availability that the triangle of authentic data are raised. Blockchain and digital signature in SCM. Blockchain and digital signature technologies have become increasingly important in supply chain management in recent years. The decentralized and distributed nature of blockchain technology provides a secure and transparent way to capture every movement of goods throughout the supply chain, while digital signatures enable the authentication of transactions and the verification of

the parties involved. This study aims to explore how blockchain technology works with digital signatures to protect the documents of organizations and one step towards enhancing sustainability and traceability is to play a major role in maintaining transparency. Using blockchain technology, the security covers monitoring activity or moment of every transaction. This technology helps ensure compliance with environmental regulations, prevent the circulation of counterfeit products, and ethical sourcing of materials, all of which contribute to more sustainable SCM. Blockchain can also enable the automatic execution of smart contracts, facilitate the seamless coordination of supply-chain activities and enforce sustainability-related requirements (The Effect of Blockchain Technology on Supply Chain Sustainability Performances, n.d.). Blockchain technology is an example of a technological model that enables the creation of a decentralized ecosystem in which data is not controlled by third parties (Ibrar Ahmed, Shilpi, 19, 2018). In CBT, cryptography is a method applied for security purposes in every sector; it doesn't matter how much capitalization a company is less or more, but security plays an essential role as a backbone to achieve more achievements in the computational world. Cryptography runs on two core keys: the public key used by the sender (user A) and the private key used by the receiver (user B). When exploring the digital signature concept for maintaining the CIA model for security purposes behind the scenes, the two keys work very efficiently. Digital fingerprints and digital signatures have the same characteristics. The digital signature is in the form of an encoded message; the signer connects to encrypt a document in a transaction that is recorded in a block, or records all transaction copies that connect in the blockchain, and maintains every history or transaction activity in an immutable form. Each recorded block is a subset of blockchain technology. The digital signature scheme often includes two algorithms: one for signing with a private key and one for validating the user's signature with users. Recent studies discuss the core synchronization using a private and public key between two users. When the user-A encrypts the message, he uses the public key of the second user, and other hand, when the user-B decrypts the message, he uses the private key. With the advancement of IT in recent times, IT has had a tremendous impact on communication with advanced security. Security is a critical aspect that will resolve different vital problems in supply chain management with advanced solutions. An electronic or digital signature accounts for 17% of the world's GDP (Dzhangarov and Suleymanova, 2020:6). Various supply chain operations mostly use an electronic document management system that supports e-signature in supply chain operations (Makale Kabul Tarihi, 2022). Now, the traditional method will be transformed into an immutable ledger that is BCT.

A. Objective

1. To study of blockchain technology and analysis of every factor of existing system

2. To identify the key challenges and barriers to adopting blockchain in SCM.

3. To evaluate the impact of blockchain on supply chain efficiency, security.

4. To analyze case studies where blockchain has been successfully implemented in SCM.

5. To propose a framework for integrating blockchain into existing supply chain systems.

B. Scope of Work

The scope of work is very essential part of research. It focuses on study, analysis and designing phase of supply chain management system (SCM) using blockchain technology, that helps to improve transparence, traceability, immutability, automation and security at a every stage with emerging algorithm. The primary stage study to make distributed system for SCM to record every activity, validity and sharing supply chain transactions among manufacturers, suppliers, logistic provider, distributor and end consumer. All participants are elements of SCM to complete the chain in a network.

This study's goal is to cover the integration of blockchain architecture components, that also integrate the distributed ledgers, consensus algorithm mechanisms, smart contract (condition or policies), cryptographic security technique. It will execute through the BCT lifecycle. Smart contract always use for the authomation means verify the any entity in system or network, that maintain the ownership as well as originality of anything. The scope includes permission-based and hybrid blockchain frameworks to control misuse of data, fraud and unauthenticated person's interruption.

The work focuses on all kind of transaction in SCM have to record in decentralized manner and using blockchain the system will strong than traditional system.

II. PROPOSED METHODOLOGY

The idea proposed that blockchain is an advanced distributed database system of all transactions are stored in the blockchain mechanism. Every block or machine connects in a chain. It maintains transparency, integrity through the chain system, and also shares data across the whole network. No one can change or break any block without permission. Blockchain reduced such conflicts by creating a decentralized, tamper-proof system that helps to store transactional records. The blockchain creates buyers and sellers. All transactions should be approved to make a successful transaction and automate updates in both ledgers in real-time. The properties of blockchain technology have led to its use in numerous sectors, like private and government, with advanced algorithms.

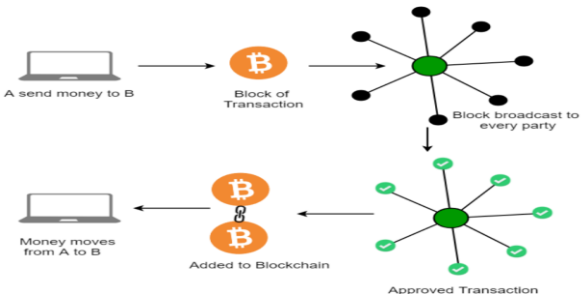

Fig: Distributed Blocks with the Blockchain Technology (https://www.geeksforgeeks.org/ethical-hacking/blockchain-technology-introduction/).

A. Cryptography:

Cryptography is a method to convert an original message to an unreadable format. It involves codes and ciphers to protect sensitive information from unauthorized persons. Cryptography is a way to secure confidential data in many applications, including banking, businesses, military communication, and so on, to secure their emails. Cryptography is one of the best solutions because it provides a very efficient way to protect private transactions between authenticated users. It enables secure transmission over the Internet.

Using private and public keys. Cryptography mainly focuses on integrity, confidentiality, and non-reputationally.

B. Encryption:

Encryption is the technique that is used to convert the original message into a complex (cipher) form. It is the process of scrambling the information to prevent another person from comprehending the message, even if it is interrupted. There is a mathematical process to convert the actual message into different formats.

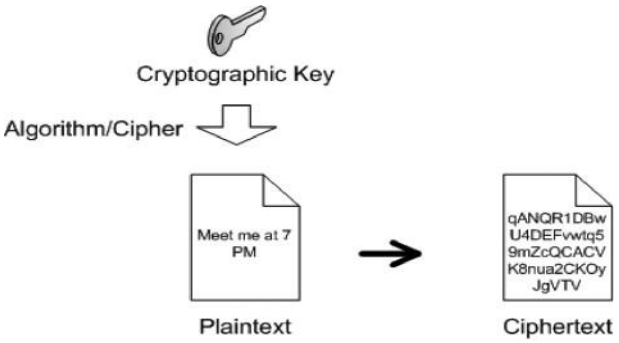

Fig: Message Encryption Process (https://www.sciencedirect.com/topics/computer-science/cryptographic-mechanism).

C. Decryption:

The next phase is the decryption process. Decryption is a process that is the opposite of encryption. In this, the complicated message will transform into a readable(original) message. The purpose of decryption is to extract the original data from the transformed message. Nobody can guess the secret message.

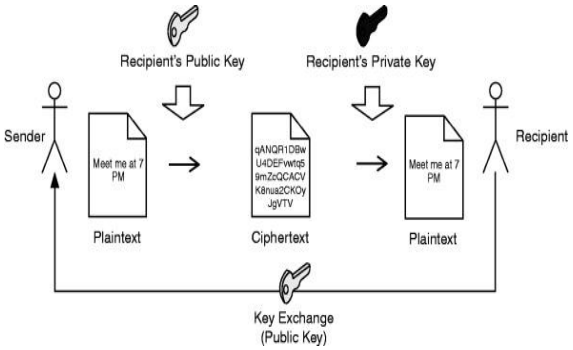

Fig: Message Decryption process (https://www.sciencedirect.com/topics/computer-science/cryptographic-mechanism).

D. Key:

A key is a piece of information that determines the output of a cryptographic algorithm. It is a critical element also authorized for use for both sides of encryption and decryption, ensuring the confidentiality, integrity and authenticity of authenticate data. Essentially, without the correct key, encrypted data cannot be properly decrypted, making it unreadable to unauthorized parties. The keys can be symmetric, where the same key is used for both encryption and decryption or asymmetric, where a pair of public and private keys is used.

E. Cipher Text:

It is a method that helps to encrypt and decrypt the plaintext in cryptography. It's a set of algorithms applied to the original message or plaintext to transform it into an understandable format to protect the sensitive information of an authenticated person.

F. Hash Function Algorithm:

A Hash function is also a cryptographic algorithm that takes an input (original message) and a fixed-size string of characters, typically a collection of letters, numbers, and symbols. The hash uniquely represents the data and is used to link blocks together. Users can encrypt various types of data using the hash function. No need for a specific format file to send.

Timestamp: That indicates the current time in seconds in universal time.

nBits: It is the target threshold of a valid block hash.

Nonce: This is a 4-byte field that starts with 0 and increases for every hash calculation.

Parent Block Hash: It shows a 256-bit hash value that points to the previous block.

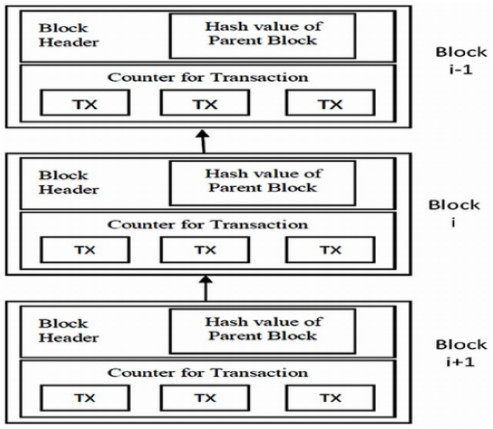

Fig: Connected Block with Hash Function.

The diagram describes how the blockchain is built by linking individual blocks together in a secure chain form. A blockchain block (e.g., Block i-1, Block i, Block i+1) that consists of a header containing metadata, the hash of the preceding block and a set of transactions. Each block connects to the others and its previous one guarantees that any alteration becomes instantly noticeable (that is not possible of alteration), rendering the data practically tamper-proof. This structural design upholds the blockchain's integrity, enhances transparency and strengthens trust within the network.

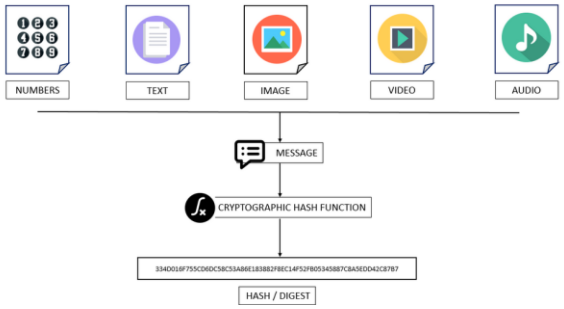

Fig: Multiple files converted with the digital signature.

The above diagram shows all the processes of creating a cryptographic hash from different types of digital data, including numbers, text, images, videos as well as audio files. All these data types are first converted into a single input, referred to as a message, which is then processed through a cryptographic hash function. This function applies a complex mathematical algorithm to the message,

producing a unique fixed-length string known as a hash or digest.

G. Digital Signature:

A digital signature means an electronic signature based on cryptography. It is a technique used to verify digital documents and the data. The digital signature follows the reverse method, which is best for maintaining strong security. When the actual user encrypts the plaintext using the private key of the sender, it is decrypted with the receiver's public key, because the keys are linked, decoding it with a public key verifies that the private key at every stage.

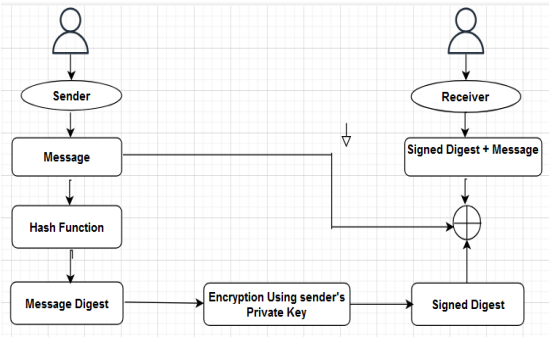

Fig: Transmission using Digital Signature

H. Certificate Authority:

The certificate authority is an entity that creates an authenticated document when an authorized administrator signs on a specific entity or certificate.

I. Digital ID:

A digital ID is the equivalent of an individual identity card. An ID can be presented electronically to prove identity. Every digital object gets an ID to share the certificate with various users.

I. Digital Certificates:

A digital certificate is any kind of document that has been converted into an electronic format. That format is known as a digital certificate because an authorized person signs it. No one can copy without permission.

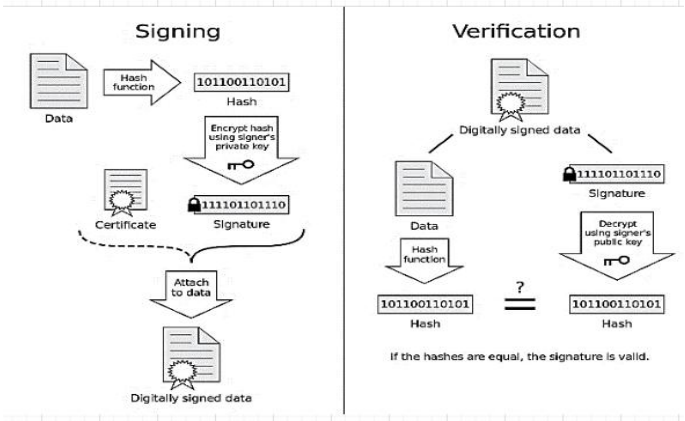

Fig: Behind the process of a private key (https://doi.org/10.21276/ijircst.2021.9.3.7).

K. Public Key Infrastructure:

Public Key Infrastructure (PKI) is a comprehensive structure that enables secure data exchange through the use of asymmetric cryptography, which involves two logically related keys: primary is a public key and the secondary is a private key. The public key is openly shared, allowing anyone to encrypt information or verify digital signatures, while the private key is kept confidential by its owner and is used to decrypt messages or create digital signatures. PKI also includes the use of digital certificates, issued by trusted entities known as Certificate Authorities (CAs) or recommended authorities, which verify the legitimacy of users, devices, or organizations

L. Private Key Infrastructure:

In contrast, Private Key Infrastructure (PKI), often referred to as a symmetric key system, employs a single secret key and it uses to one of the shared secret key for both encryption and decryption. Exactly by the opposite side of the asymmetric approach, it does not use public keys or digital certificates. Therefore, the security of this method depends on maintaining the secrecy of the shared key. While symmetric key concepts are relatively simple to implement and perform efficiently in small-scale or closed network settings, they face limitations in scalability and are more liable to breaches since the exposure of a single key can compromise the entire system.

RESULT

In the modern era, the increasing frequency of cyberattacks poses a significant risk to data security, operational stability and overall business performance across industries. Research findings indicate that integrating blockchain technology with digital signatures provides a robust framework for upgrading cybersecurity and ensuring the authenticity of digital data. Within the manufacturing sector, adoption of digital signature solutions has led to more efficient and streamlined operations across areas such as product design, production management, marketing, sales and many more.

Moreover, the use of digital signatures is considered to reduce paperwork and administrative delays, while getting transparency, efficiency and trust across the environment of SCM. This integration also reinforces the security, integrity and legal validity of digital documents within blockchain-based systems and transactions, thereby facilitating very smoother global trade and ensuring contractual reliability in international business operations.

The adoption of digital signatures has also been observed to significantly decrease paperwork and administrative delays, lowering operational costs while improving transparency, traceability and trust throughout the production and supply chain. Additionally, this approach strengthens the security, integrity and legal enforceability of digital documents in blockchain networks and transactions, supporting smoother global trade and maintaining contractual reliability in global operations.

CONCLUSION

This study focuses on understanding real user needs in specific application areas, especially in SCM. In this field, cryptography plays a key role in keeping data secure and building trust within the system. Blockchain technology provides an advanced way to protect transactions across different industries, such as banking, healthcare and finance. The use of a digital signature strengthens blockchain security and supports its use in both research and real-world applications.

Decentralization is another important feature, as it helps protect all nodes in the blockchain network. The introduction of digital signatures has greatly improved the digitalization of supply chain processes, making operations faster and more efficient. This has also reduced the complexity of traditional, time-consuming procedures. Decentralization enhances important qualities like authenticity, integrity and non-repudiation, which are essential for ensuring data transparency and trust.

Furthermore, using digital signatures supports sustainability by reducing paper usage and lowering the carbon footprint in supply chain activities. With these advantages, the authentic digital signature is becoming more essential in SCM and reliable digital transactions in the future.

REFERENCES

Ahmad, F. A., Kumar, P., Shrivastava, G., & Bouhlel, M. S. (2018). *Bitcoin: Digital decentralized cryptocurrency.* In Handbook of research on network forensics and analysis techniques (pp. 395–415). IGI Global. https://doi.org/10.4018/978-1-5225-4100-4.ch021Gudumian, S., Lizy, A., Jagadeeswari, S., Chinnadurai, S., Kesavan, T., & Gopi, R. (2024). Enhancing safety solutions through blockchain technology and digital signatures.

Bacchetta, A. V. B., Krümpel, V., & Cullen, E. (2021). *Transparency with blockchain and physical tracking technologies: Enabling traceability in raw material supply chains* (p. 1). https://doi.org/10.3390/materproc2021005001

Bolfing, A. (2021). *Cryptographic primitives in blockchain technology: A mathematical approach.*

Dong, S., Shi, W., Abbas, H., Li, Z., & Kamruzzaman, J. (2023). *Blockchain technology and application: An overview.* PeerJ Computer Science, 9, e1604. https://doi.org/10.7717/peerj-cs.1604

Gudumian, S., Lizy, A., Jagadeeswari, S., Chinnadurai, S., Kesavan, T., & Gopi, R. (2024). *Enhancing safety solutions through blockchain technology and digital signatures.*

Katz, J., & Lindell, Y. (2020). *Introduction to modern cryptography* (3rd ed.). Boca Raton, FL: CRC Press.

Nalayini, C. M., & Katiravan, J. (2022). *Detection of DDoS attacks using machine*

learning algorithms. Journal of Emerging Technologies and Innovative Research, 9(7).

Pachghare, V. (2019). *Cryptography and information security.* Noida, Uttar Pradesh, India: PHI Learning Pvt. Ltd.

Simplilearn. (n.d.). *What is cryptography?* Retrieved from https://www.simplilearn.com/tutorials/cryptography-tutorial/what-is-cryptographys

Song, J. M., Sung, J., & Park, T. (2019). *Applications of blockchain to improve supply chain traceability.* Procedia Computer Science, 162, 119–122. https://doi.org/10.1016/j.procs.2019.11.266

The effect of blockchain technology on supply chain sustainability performances. (n.d.). https://doi.org/10.3390/su13041726

Trends in data protection and encryption technologies. (2022). *Open Access Repository.*

Viand, A., Knabenhans, C., & Hithnawi, A. (2023). *Verifiable fully homomorphic encryption.* arXiv Preprint arXiv:2301.07041.

https://www.fortinet.com/resources/cyberglossary/digital-certificates

Kamble, S., Patil, R., & Shinde, P. (2023). Verification of ownership using blockchain in IP management systems. *International Journal of Computer Applications, 25*(6), 45–54. https://doi.org/10.1109/COMPSAC.2018.10258

Saaty, T. L. (1980). *The analytic hierarchy process: Planning, priority setting, resource allocation.* McGraw-Hill.

Finck, M., & Moscon, V. (2018). Copyright law on blockchains: Between new forms of rights administration and digital rights management 2.0. *IIC – International Review of Intellectual Property and Competition Law, 50*(1), 10.1007/s40319-018-00776-8.

Gürkaynak, G., Yılmaz, İ., Yeşilaltay, B., & Bengi, B. (2018). Intellectual property law and practice in the blockchain realm. *Computer Law & Security Review, 34*(4), 847–862. https://doi.org/10.1016/j.clsr.2018.05.027

Halloush, Z., & Yaseen, Q. (2019). A blockchain model for preserving intellectual property. *Proceedings of the 2019 International Conference on Computing and Information Technology*, 1–5. https://doi.org/10.1145/3368691.3368744

https://www.sciencedirect.com/topics/computer-science/cryptographic-mechanism

https://doi.org/10.21276/ijircst.2021.9.3.7