A Review on Preserving Data Confidentiality in Blockchain-based IoT-Supply Chain Systems

Omimah Alsaedi[1†,] Omar Batarfi[2††], Mohammed Dahab[1†],
oalsaedi0003@kau.edu.sa obatafri@kau.edu.sa mdahab@kau.edu.sa
[†]Department of Computers Science, King Abdulaziz University, Saudi Arabia
[††]Department of Information Technology, King Abdulaziz University, Saudi Arabia

Abstract
Data confidentiality refers to the characteristic that information kept undisclosed or hidden from unauthorized parties. It considered a key security requirement in current supply chain management (SCM) systems. Currently, academia and industry tend to adopt blockchain and IoT technologies in order to develop efficient and secure SCM systems. However, providing confidential data sharing among these technologies is quite challenging due to the limitations associated with blockchain and IoT devices. This review paper illustrates the importance of preserving data confidentiality in SCM systems by highlighting the state of the art on confidentiality-preserving methodologies in the context of blockchain based IoT-SCM systems and the challenges associated with it.

Keywords:
Blockchain, Supply Chain, SCM, IoT, Confidentiality

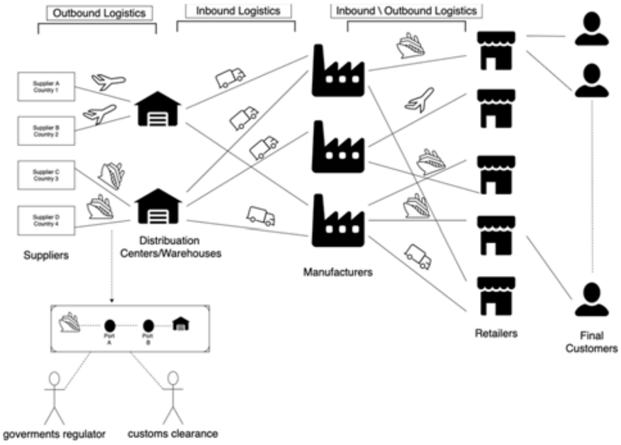

Figure 1:Global supply chain with inbound and outbound logistics

1. Introduction

Supply chain can be defined as a network of all participating entities in producing a product from the stage of sourcing raw materials to delivering the final product. This may include resources and activities, along with physical and informational flow [1].

Currently, Supply chains operate under a growing and ever-changing environment. A main factor that can influence the supply chain can be, out of other possible causes. These businesses involve a growing number of participants who share a large amount of information over different geographical areas [2], resulting in sophisticated supply chain managements which makes managing supply chain operations more complex as illustrated in Figure 1. Therefore, academia and industrial communities tend to digitize supply chain management (SCM) systems through implementing advanced technologies such as IoT, cloud computing, artificial intelligence, and blockchain technology.

IoT is a communication paradigm that allows various kinds of objects to interconnect together to collect and share data using the internet [3]. IoT objects refer to anything that can be connected to the Internet through embedded computer chips and sensors such as buildings, cars, phones, and wearable devices.

In fact, Integrating IoT devices with SCM systems allow different objects to sense and monitor data such as location, temperature, and motion in a real-time manner across different supply chain phases, offering enhanced visibility, traceability, and information sharing between supply chain stakeholders, therefore, it leads to optimized planning and controlling of supply chain processes and resources [2]. However, integration of IoT technologies such as Radio Frequency Identification (RFID) tags and sensors opens the opportunity for several security attacks since IoT devices are owned by different parties and collect a great amount of data that is uploaded to the internet and managed in a centralized manner which affects data integrity, availability, and confidentiality. Moreover, IoT devices are heterogeneous by nature, with limited storage, energy, and computing size. Therefore, protecting IoT-based systems requires suitable security approaches.

Recently, due to the unique characteristics of blockchain technology, it is introduced as the missing piece of the puzzle to settle IoT-SCM system security, reliability issues[4]

Blockchain is defined as a decentralized peer-to-peer network that allows peers to manage transactions, value,

Manuscript received November 5, 2023
Manuscript revised November 20, 2023
https://doi.org/10.22937/IJCSNS.2023.23.11.14

and assets without the need for intermediaries. The decentralization and immutability features of blockchain enhances availability and integrity, yet the high transparency of blockchain reduces data confidentiality which considered one of the key security requirements that maintain supply chain sustainability.

This paper highlights the importance of preserving data confidentiality in IoT-SCM systems and reviews the current state of the art confidentiality-preserving methodologies in the context of blockchain based IoT-SCM systems and the challenges associated with it.

The rest of the paper is organized as follows: Section 2 reviews some related work presented in the same scope as our review. Section 3 describes the basic knowledge regarding the main component including blockchain, IoT, and supply chain. Section 4 identifies the main research problem. Section 5 review the available methodologies proposed in the literature to solve the addressed problem.

Section 6 identifies and discusses the main challenges and implications, before the conclusion is presented in Section 7.

2. Related Work

Abylay and mariusz [5] have reviewed several privacy-preserving techniques associated with blockchain and categorized the main techniques examined into three categories: identity data anonymization, privacy preservation of smart contract, and transaction data anonymization, Moreover, they have identified the main applications of blockchain where the privacy protection is a fundamental requirement.

Cha et al. [6] and zhang et al. [7] have addressed the current solutions for data protection in the blockchain. They focused on analyzing the usability and the efficiency of the different cryptography-based solutions including symmetric and asymmetric encryption, Key-Policy Attribute-Based Encryption (KP-ABE), Ciphertext-Policy Attribute-Based Encryption (CP-ABE), and shared secret. Consequently, the associated challenges have been addressed and future research directions have been defined as they have stated that the current solutions are still far to cope with the addressed challenges especially in complicated applications such as IoT.

In contrast, iftikhar et al. [8] have investigated the exciting data privacy mechanisms for IoT devices using blockchain, they have pointed out the advantages and the limitations of each machine along with the related challenges that should be taken into account in future research. Rouhani [9] has presented a state of the art on using access control mechanisms for protecting blockchain data and the related challenges.

The main contribution of this paper is to highlight the current state of the art of protecting data and preserving confidentiality in the context of blockchain-based IoT-SCM systems.

3. Main Components

In this section, we provide a basic knowledge about the main component of our review including Blockchain, Internet of Things, and Supply chain.

3.1. Blockchain

In 2008, Satoshi Nakamoto proposed the first decentralized peer-to-peer electronic cash system - called Bitcoin, which form the basic idea that led to the appearance of blockchain (BC) technology [2].

Blockchain is defined as a distributed, appended-only ledger of transactions that are added into a network in the form of digital blocks. Figure 2 illustrates block structure in the blockchain network.

Blocks are chronologically ordered in which each block is connected to the preceding block through a cryptography hash function.

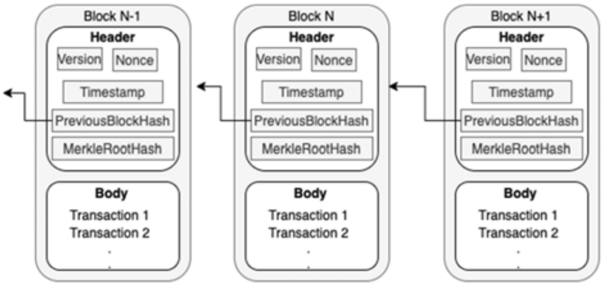

Figure 2: Blockchain Architecture

Basically, a blockchain network consists of numerous nodes sharing the same administrative role and storing the same copy of data, there is no centralized authority over the network in which each node can update the distributed ledger by adding a transaction, and each set of transactions are stored on connected blocks. However, each block is consisting of the block header that includes the metadata that identifies each block, block body that includes a list of all transaction within the block depending on the block size that differs from one blockchain platform to another.

The technology on which the blockchain is built has empowered it with many distinctive features which are:

- **Decentralization**: Blockchain eliminates the need for the involvement of a centralized authority or a third party to control and store the data as all nodes within the network can validate the transactions independently and store the same copy of the ledger. In the case of a node faultier, no data will be lost, and the network will remain functional as there is no single point of failure.

- **Reliability**: Although there is no centralized authority over the blockchain network, it remains reliable as each generated transaction should be digitally signed using the hashing algorithm with a private/secret key of the sender to be considered as a valid transaction [10] which ensure authenticity. In addition, every transaction within the network is validated from each node using some consensus protocol to be added to the ledger [11]. This mechanism provides trust and ensures ledger consistency among the distributed network.
- **Immutability:** Hashing is a backbone of the blockchain technology, every block is connected the previous block through its hash except the first block in the chain (genesis block) that points to itself [12], the add-only structure, and this kind of feature make the blocks chronologically connected, changing one block will require to change all proceeding blocks on all participating nodes. As a result, changing or modifying the ledger is almost impossible, which enhances the integrity of the data.
- **Transparency**: all performed transactions are stored on each node with the related data and hash value, which make the ledger visible, and audible by all the nodes within the network [10].
- **Anonymity:** blockchain allows to generation of an anonymous set of numbers as a node address. Hence, any node can participate in the network without revealing its original identity [12].

3.2. Internet of Things

Internet of Things (IoT) is a communication parade that allows different kinds of objects to interconnect together to collect and share data using the internet [3][13] Objects refer to anything that can be connected to the internet through embedded computer chips and sensors such as people, buildings, cars, phones, and wearable devices. IoT reshapes the communication between heterogeneous objects with different characteristics such as power and capacity by allowing them to directly communicate and interact with each other rapidly and in a real time manner without human intervention.

Basically, IoT ecosystem consists of a number of major components that can be described as its building blocks [14], which include the physical devices, the network infrastructure, the cloud infrastructure, and the gateway that act as an intermediate between the devices and the cloud, in addition to a different software and hardware components that integrated into the IoT ecosystem depending on the context of use, in order to provide an efficient IoT solution that achieves the desired functionality and security.

Although integrating IoT devices will effectively enhance the collaboration and visibility among different applications, the heterogeneous nature of the large scale connected IoT objects that have different characteristics and deal with a large amount of critical data open the opportunity for attackers to manipulate the IoT system from different aspects, which results in many security concerns that affect data integrity, availability, and confidentiality [3].

In fact, security remains a challenge since IoT devices are lightweight with limited storage, energy, and computing size. These devices must devote most of their power and computation to executing core application functionality [15] . Therefore, the traditional security methods are not suitable for preserving IoT security because of the energy consumption and processing overhead related to these methods. Hence, it is necessary to keep these factors in mind when choosing an appropriate security approach for IoT-based systems.

3.3. Supply chain

The Supply chain is a complex and dynamic system that evolves over time. Products movements across the network to transform the raw material into a final product is not a straightforward process.

Figure 3 illustrates the physical and the information flow between supply chain entities.

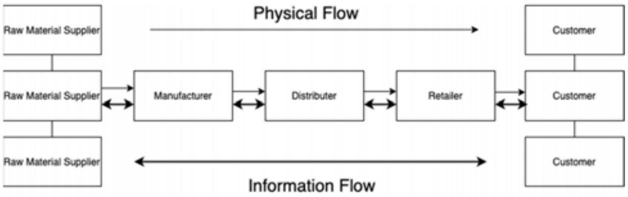

Figure 3 Supply Chain Flow

In fact, supply chain can be found in roughly every business regardless of its type or size. Consequently, the practice of SCM comes into life, which concerns the active planning and controlling of supply chain activities to maximize customer value and achieve a sustainable competitive advantage [12]in an efficient and effective manner. It involves delivering the right product in the right condition, in a timely manner, and at the minimum possible cost.

SCM originally used the traditional paperwork to trace the movement of product, finance, and information [16]. Lately, because of the digital evolution and business growth, the traditional supply chain transformed into Digital Supply Chain (DSC) which refers to integrating IT infrastructure and technologies to connect and share product data in a virtual network [17].

In fact, the traditional supply chain may provide a relatively safe environment for the information, but it is no longer effective under the increasing networks that require safe, fast, and low-cost solutions.

In contrast, DSC has a huge impact in providing an effective supply chain by facilitating the process of collecting, analyzing, storing, sharing, and auditing data in a real-time manner. Yet it has several risks associated with it because it is connected to the unstable internet environment that may contain additional or intermediate parties such as IoT devices or cloud storage, which makes it vulnerable to the various attack that leads to real problems [1].

4. Confidentiality in Blockchain-based IoT-SCM systems

Confidentiality in a supply chain refers to the exchange of information between partners inside the supply network, but not with outsiders [18]. Interconnected organizations across the network are in charge of preventing others from accessing the information. In fact, one of the main threats in SCM systems is the unauthorized access and illegal data disclosure that affect the confidentiality of sensitive information shared between supply chain stakeholders. Recently, several data breaches have been reported. It affected not only the personal and financial data of the company itself, but also affected its partners, suppliers, and customers [19].

On the other hand, there is a dilemma between transparency and confidentiality of data inside IoT-SCM systems, blockchain provides an ideal solution to improve the transparency of the shared data, yet it is inefficient to achieve full transparency over the supply chain as only a part of data need to be shared to achieve the balance between the degree of data transparency that positively affects the business value and the confidentiality level required to the sensitive data that should be visible only to selected stakeholders in order to protect personality, intellectual property, and the business competitiveness [20][21].

In an investigation of some logistics operator and business managers opinions regarding the confidentiality and transparency requirements of their supply chain, almost all of them have stated that they prefer to keep specific information confidential and private to a select domain within the supply chain such as customers information, goods prices, and intellectual property-related information [21]. In fact, the strong security aspect that is associated with blockchain structure is considered the key driver behind adopting this technology in different applications as it can enhance several security requirements such as integrity and availability. However, data confidentiality is not guaranteed by blockchain since its structure provides a high level of transparency among its network participants, in which all transactions are visible to everyone who has access to the network. Although private blockchain is considered more confidential as it is more restrictive than public blockchain in which it allows only pre-selected participants to access and view data, achieving confidential data sharing in SCM systems requires limiting the visibility of some transactions to only a subset of organizations within the network.

5. Preserving Data Confidentiality in Blockchain-based IoT-SCM systems

In this section, we review the different methodologies proposed in the literature to ensure the confidentiality of data in blockchain-based IoT-SCM systems.

5.1. Encryption

Encryption is a common approach used to preserve data confidentiality. It refers to the process of disguise data by transforming human-readable plain-text into an unreadable format called cipher-text, using a specific mathematical-based cryptographic algorithm that involves the use of a special cryptographic key to encrypt and decrypt data. Several researchers have proposed different cryptography approaches to protect data in blockchain-supply chain management systems.

The work of Maouchi et al. in [20] applies the Elliptic Curve Integrated Encryption Scheme (ECIES) on the part of each transaction that holds the sensitive data in their blockchain-based SCM system. Sensitive data is encrypted along with a set of authorized recipients public keys. Later, each actor in the network attempts to decrypt the cipher-text, if he is an authorized user, the data is retrieved.

In the IoT-based pharmaceutical supply chain management system proposed by Jianfeng et al. [22], both symmetric encryption algorithm and asymmetric encryption algorithm Rivest-Shamir-Adleman (RSA) were implemented through blockchain smart contract in order to encrypt both sensitive data and encryption key respectively as follow:

- Organization A generates an encryption key that is encrypted by the public key of the authorized recipients(s)

$$Ckey = RSA\text{ (Key,PU)} \tag{1}$$

- The sensitive data itself is encrypted by Organization A using symmetric encryption algorithm (ENC)

$$Encrypted - Data = ENC\text{ (Data,PU)} \tag{2}$$

Both Ckey and Encrypted-Data are stored in the blockchain. To decrypt data by the authorized recipient:

- The recipients need to obtain a key first using its private key

$$Key = DRSA\text{ (Ckey-Data,PV)} \tag{3}$$

- Then decrypt the data using the key

$$Data = DENC\text{ (Encrypted-Data,Key)} \tag{4}$$

The work of Yang et al. in [23] divided supply chain data into public data that is stored using an off-chain MySQL database, and private data that is encrypted using Cipher Block Chaining (CBC) mode of the Advanced Encryption Standard (AES) algorithm and stored on chain along with the hashes of the public data to maintain its integrity. Moreover, a second encryption is performed using Elliptic Curve Cryptography (ECC) to encrypt the generated encryption key of the private data encryption process and stored on-chain. In fact, both encryptions are performed on smart contract level. As a result, to obtain the private data, authorized node needs to perform a two-steps decryption to decrypt both the key and private data.

5.2. Access Control

Access control is a security technique that governs who has access to system resources by imposing predetermined access control policies [9]. In blockchain-based SCM systems, different data-sharing access control methods have been enforced in order to limit the visibility over the sensitive data and offer the required traceability without affecting data confidentiality.

Flapper in [24] proposed a conceptual framework that uses an XML-standard version to manage and perform Attribute-Based Access Control (XACML) that limit access to confidential data to authorized nodes only, in a distributed manner using Ethereum smart contract. Also, he integrates BigchainDB blockchain to serve as a additional database to store assets data and access control policies.

A declarative access control method is implemented in [25]to determine the authorization of supply chain stakeholders to read, write, and update elements using blockchain. In fact, the authors have used Ethereum smart contract to store both user info and order data access path. Besides, an InterPlanetary File System is used to store the data itself. Moreover, a network communication module is used to store communication-related data in order to enhance the overall storage capacity by storing only order-related data on the blockchain.

5.3. Multi-Channel Network

A channel is a key part of any blockchain network in which different members communicate and interact with one another. Each channel is defined by members (organizations), anchor peers, a shared ledger, and a smart contract.

Basically, each transaction on the network is executed on a channel in which it can be seen by all its members. However, in order to carry out private and confidential transactions, Kurniawan in [26] focuses on providing a private data sharing approach through limiting the access of sensitive data to a subset of supply chain organizations. Particularly, the Hyperledger-based system implements multiple channels within the blockchain network in which each channel has its own ordering node, organizations nodes, and a shared ledger between them. Each organization node may be involved in multiple channels, and each channel may have multiple nodes sharing exclusive data that is not visible to other members outside the channel. Additionally, the system has a channel that includes all nodes in the network to store other public data.

Similarly, Surjandari et al. in [27] have proposed a multi-channel blockchain-based framework to implement a secure and confidential halal food supply chain. The proposed framework consists of three separate channels that combine supplier and producer, producer and distributor, distributor, and end-user respectively in which each channel is completely isolated from the other channels. However, having no channel that combines all supply chain stakeholders leads to inefficient SC traceability as each participant is allowed to track part of the product history. Hence, this solution decreases transparency and increases the fraud rate.

6. Discussion

Reviewing the proposed literature has led us to observe the limitations and the challenges related to the presented methodologies. In this section we highlight these challenges.

Performance and Storage Scalability: scalability refers to the ability of a system to scale up with additional resources and demand to cope with the changing needs without being affected negatively in terms of storage or performance. In terms of SCM, a single product may require up to 200 communication processes to achieve a successful delivery from source to destination [28]. Furthermore, a single process could include several documents, invoices, properties, and specifications. Integrating such systems with the constrained IoT devices that collect huge amounts of data requires a storage structure that is suitable for storing a big volume of data. In addition to the size of the data itself, the space complexity is increased by the amount of encrypted data.

On the other hand, protecting and disseminating the cryptographic key among the authorized peers requires additional effort besides the additional performance overhead related to the encryption and decryption processes. Therefore, performing smart contract level encryption in blockchain-based IoT-SCM is not efficient since blockchain is not an appropriate structure for storing and processing large amounts of data.

System Complexity: managing supply chain entities and operations is not a straightforward process which makes SCM systems complex by nature. Adopting multiple channels blockchain architecture to achieve confidential data sharing leads to increased system complexity and limited traceability since every single node could have more than one ledger and need to access multiple channels to trace and retrieve a single product private and public data.

Off-chain Storage Security: adopting on-chain and off-chain storage structures in blockchain-based IoT-SCM systems is urgently needed in which the large, less secure, and public data is stored off-chain while it hashes are stored on-chain in order to benefit from the features afforded by the blockchain, while the sensitive data could be stored off-chain or on-chain. The idea is to limit the amount of data that is stored and processed on-chain wherein the confidentiality solutions are applied to a fewer amount of data. Several solutions have implemented the hybrid storage structure, some of these solutions have chosen to store the private data on-chain along with the hashes that point to the public data that stored externally, whereas other solutions have stored both private and public externally and maintain only the hashes on-chain and link the hashes with the physical storage location. The challenge, then, is to provide convenient security mechanisms to protect the off-chain storage data from unauthorized access and deletion.

7. Conclusion and Future Work

In this paper, we explained the basic concepts related to Blockchain, Internet of Things, and Supply Chain Management Systems. Moreover, we showed how integrating IoT and blockchain technologies can effectively enhance SCM systems functionality and security. Yet most of the current schema lacks the ability to provide data confidentiality. The currently available methodologies to preserve data confidentiality in blockchain based IoT-SCM systems are reviewed, and the key challenges associated with it are highlighted in this work.

In our future work, we plan to analyze the requirements of blockchain based IoT-SCM systems and implement a confidential data sharing mechanism that fits these requirements to overcome the stated challenges.

References

[1] J. Zhang, H. Chen, L. Gong, J. Cao, and Z. Gu, “The current research of IOT Security,” 2019 IEEE Fourth International Conference on Data Science in Cyberspace (DSC), 2019.

[2] M. Ben-Daya, E. Hassini, and Z. Bahroun, “Internet of things and supply chain management: a literature review,” International Journal of Production Research, vol. 57, no. 15–16, pp. 4719–4742, Nov. 2017, doi: 10.1080/00207543.2017.1402140. [Online]. Available: http://dx.doi.org/10.1080/00207543.2017.1402140

[3] P. Urien, “lockchain IoT (BIoT): A New Direction for Solving Internet of Things Security and Trust Issues,” 2018 3rd Cloudification of the Internet of Things (CIoT), pp. 1–4, 2018, doi: 10.1109/CIOT.2018.8627112.

[4] A. Panarello, N. Tapas, G. Merlino, F. Longo, and A. Puliafito, “Blockchain and IoT Integration: A Systematic Survey,” Sensors, vol. 18, no. 8, p. 2575, Aug. 2018, doi: 10.3390/s18082575. [Online]. Available: http://dx.doi.org/10.3390/s18082575.

[5] A. Satybaldy and M. Nowostawski, “Review of techniques for privacy-preserving Blockchain Systems,” Proceedings of the 2nd ACM International Symposium on Blockchain and Secure Critical Infrastructure, 2020.

[6] J. Bernal Bernabe, J. L. Canovas, J. L. Hernandez-Ramos, R. Torres Moreno, and A. Skarmeta, “Privacy-preserving solutions for Blockchain: Review and Challenges,” IEEE Access, vol. 7, pp. 164908–164940, 2019.

[7] R. Zhang, R. Xue, and L. Liu, “Security and privacy on Blockchain,” ACM Computing Surveys, vol. 52, no. 3, pp. 1–34, 2020.

[8] Z. Iftikhar, Y. Javed, S. Y. Zaidi, M. A. Shah, Z. Iqbal Khan, S. Mussadiq, and K. Abbasi, “Privacy preservation in resource-constrained IOT devices using blockchain—A survey,” Electronics, vol. 10, no. 14, p. 1732, 2021.

[9] S. Rouhani and R. Deters, “Blockchain based access control systems: State of the art and Challenges,” IEEE/WIC/ACM International Conference on Web Intelligence, 2019.

[10] R. Gupta, Hands-On Cybersecurity with Blockchain. Packt Publishing Ltd, 2018.

[11] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, “An overview of blockchain technology: Architecture, consensus, and future trend,” 2017 IEEE International Congress on Big Data (BigData Congress), pp. 557–564, 2017, doi: 10.1109/BigDataCongress.2017.85

[12] N. Vyas, A. Beije, and B. Krishnamachari, Blockchain and the Supply Chain. Kogan Page Publishers, 2019.

[13] M. Son and H. Kim, “Blockchain-based secure firmware management system in IOT environment,” 2019 21st International Conference on Advanced Communication Technology (ICACT), 2019.

[14] N. M. Kumar and P. K. Mallick, “The internet of things: Insights into the building blocks, component interactions, and architecture layers,” Procedia Computer Science, vol. 132, pp. 109–117, 2018.

[15] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, “Blockchain for IOT security and privacy: The case study of a smart home,” 2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops), 2017.

[16] H. Peck, “Reconciling supply chain vulnerability, risk and supply chain management,” International Journal of Logistics Research and Applications, vol. 9, no. 2, pp. 127–142, 2006.

[17] G. E. Smith, K. J. Watson, W. H. Baker, and J. A. Pokorski II, “A critical balance: Collaboration and security in the IT-enabled Supply Chain,” International Journal of Production Research, vol. 45, no. 11, pp. 2595–2613, 2007.

[18] L. Li and H. Zhang, “Confidentiality and information sharing in Supply Chain Coordination,” Management Science, vol. 54, no. 8, pp. 1467–1481, 2008.

[19] B. Bhargava, R. Ranchal, and L. Ben Othmane, “Secure information sharing in digital supply chains,” 2013 3rd IEEE International Advance Computing Conference (IACC), 2013.

[20] M. El Maouchi , O. Ersoy , and Z. Erkin, “Decouples: a decentralized, unlink- able and privacy-preserving traceability system for the supply chain,” Proceedings of the 34th ACM/SIGAPP Symposium on Applied Computing, pp.

364–373, Apr. 2019, doi: https://doi.org/10.1145/3297280.3297318.

[21] A. Akram and P. Bross, “Trust, Privacy and Transparency with Blockhain Technology in Logistics,” MCIS 2018 Proceedings, vol. 17, 2018, [Online]. Available: https://aisel.aisnet.org/mcis2018/17.

[22] J. Shi, D. Yi, and Jian Kuang, “Pharmaceutical Supply Chain Management System with Integration of IoT and Blockchain Technology,” nternational Conference on Smart Blockchain, vol. 11911, pp. 97–108, 2019, doi: 10.1007/978-3-030-34083-4_10.

[23] X. Yang, M. Li, H. Yu, M. Wang, D. Xu, and C. Sun, “A Trusted Blockchain-Based Traceability System for Fruit and Vegetable Agricultural Products,” IEEE Access, vol. 9, pp. 36282–36293, 2021, doi: 10.1109/access.2021.3062845. [Online]. Available: http://dx.doi.org/10.1109/access.2021.3062845

[24] J. Flapper, “User access control on the blockchain for supply chain visibility,” thesis, University of Twente, 2019, doi: http://essay.utwente.nl/78800/.

[25] Y. Fan, X. Lin, W. Liang, J. Wang, G. Tan, X. Lei, and L. Jing, “Tracechain: A blockchain-based scheme to protect data confidentiality and traceability,” Software: Practice and Experience, vol. 52, no. 1, pp. 115–129, 2019.

[26] K. Winata, “Blockchain based Data Sharing System for Supply Chain,” INTERNATIONAL JOURNAL OF ENGINEERING RESEARCH & TECHNOLOGY (IJERT), vol. 09, no. 11, Nov. 2020, doi: 10.17577/IJERTV9IS110272.

[27] I. Surjandari, H. Yusuf, E. Laoh, and R. Maulida, “Designing a Permissioned Blockchain Network for the Halal Industry using Hyperledger Fabric with multiple channels and the raft consensus mechanism,” Journal of Big Data, vol. 8, no. 1, Jan. 2021, doi: 10.1186/s40537-020-00405-7. [Online]. Available: http://dx.doi.org/10.1186/s40537-020-00405-7

[28] H. Hellani, L. Sliman, A. E. Samhat, and E. Exposito, “On blockchain integration with supply chain: Overview on data transparency,” Logistics, vol. 5, no. 3, p. 46, 2021.

Omimah Alsaedi received the B.E. degrees, from Umm Al-Qura University in 2017. She is currently MSc student in Computer Science at King Abdulaziz University, Saudi Arabi. She works as information security analyst. Her research interests include IoT, Information Security, and Blockchain.

Dr Batarfi received his B.S. degree in Computer Science from King Abdulaziz University, Jeddah, Saudi Arabia in 1989 and his M.S. degree in Artificial Intelligence from George Washington University, Washington, D.C., USAin 1996. He received his Ph.D. from the University of Newcastle Upon Tyne, UK in 2008. From 2008 to 2016, he was an Assistant Professor with the Faculty of Computing and Information Technology, King Abdulaziz University, Jeddah, Saudi Arabia. He is currently an Associate Professor of Networking Security at Information Technology Department, Faculty of Computing and Information Technology, King Abdulaziz University, Jeddah, Saudi Arabia. His research interests include Big Data, Cloud Computing, and Information Security.

Dr Dahab is an associate professor at the Department of Computer Science in the Faculty of Computing and Information Technology, King Abdul Aziz University (KAU), Jeddah, Saudi Arabia. He served as the Chairman of the agricultural expert systems development department for 2 years at The Central Laboratory for Agricultural Expert Systems (CLAES), Ministry of Agriculture Egypt. His main research interests include pattern recognition, natural language processing, expert systems, knowledge bases and information retrieval.