Blockchain for Sustainable Supply Chain: Applications and Challenges

Conference Paper · June 2021

CITATIONS
0

READS
55

4 authors, including:

Zainab Senan Mahmod
International Islamic University Malaysia
40 PUBLICATIONS **481** CITATIONS
SEE PROFILE

Noradila Nordin
Northern University of Malaysia
10 PUBLICATIONS **62** CITATIONS
SEE PROFILE

Proceedings of International Conference on Engineering Professional Ethics and Education 2021 (ICEPEE'21)
22 – 23 June 2021, Kuala Lumpur, Malaysia.

Blockchain for Sustainable Supply Chain: Applications and Challenges

Sumayyah Bukola Adetunmbi [1], Zainab S. Attarbashi [1*], Noradila Nordin[1], and Suhaidi Bin Hassan[1]

[1]*InterNetWorks Research Lab, School of Computing, Universiti Utara Malaysia, Kedah, Malaysia*

Zainab.senan@uum.edu.my

Abstract— Sustainable supply chain can be achieved by being aware of the ecosystem's environment. Nowadays, all types of supply chains between the producer and the consumer have become complex and long. This supply chain is lacking transparency regarding the journey of the products which can result in the increase of contaminated foods. Also, there is a chance of data manipulation as the records about the foods' movement are usually digitally centralized or even paper-based. Blockchain technology can help to build secured, traceable and transparence transactions of services. With the blockchain ledger it is possible to quickly verify the location, history, and status of a particular food product and everyone can access the data. This paper is reviewing different attempts to use blockchain to manage supply chains. Then it highlights some security issues facing blockchain in recent years to have more understanding of these issues and how to address them.

Keywords: *Blockchain technology, supply chain, blockchain challenges, distributed ledger, smart contracts.*

1. Introduction

The concept of blockchain technology was first introduced some years back in the area of cryptocurrency. Due to its great success in this area, it was later introduced in various other sectors. It has been used in sectors such as banking, global finance, enterprise services and now more focus is being given to blockchain technology in the supply chain sector. Blockchain is a distributed ledger technology whereby it uses an innovative technological approach to realizing decentralized trustless systems. The blockchain ensures the security and privacy of data by indexing the identity and locations in a decentralized approach [1][2]. Blockchain is a distributed ledger that is programmed to record online transactions in a secure way that cannot be manipulated. All transactions/information are chunked into blocks and linked so that each block is linked to the previous and next blocks. Each record in this ledger is protected by cryptographic rules, making it more reliable and tamper-proof. All the records of the transactions are checked with the approval of the system's participants [3]. When adopted, blockchain cannot be reversed or refused because the agreement is carried out with the mutual consent of all parties [4]. In the blockchain, each transaction has a digital signature from participants to ensure its security and authenticity. It focuses on storing information safely and efficiently in a distributed environment so that it cannot be tampered with or compromised.

Blockchain offers numerous security characteristics that include fault tolerance, full traceability, and auditability where the block is characterized by cryptographic schemes and secure timestamp, integrity, and authorization with the use of hash function and digital signature algorithm to validate signatures. Blockchain is also transparent where the transactions are appended into blocks and replicated publicly. Even though the distributed ledger is publicly accessible, the keys relative to the parties are anonymous, thus protecting privacy.

There are three types of blockchain, public, private, and consortium which define the membership control of the consensus in a blockchain. Consensus is achieved by using the prior agreement mechanisms. The ledgers are visible to anyone of all these types. However, in consortiums, the ledger can be restricted to a selected group. In public blockchains, anyone can verify and add transaction blocks while in private and consortium blockchains, only specific people or groups of the organization (such as banks) are allowed. This has to be considered when evaluating the consensus algorithms in the blockchain design based on the membership control that fits the nature

of the business application [5][6]. A good consensus algorithm means efficiency, safety, and convenience [7]. Several consensus algorithms that have been employed in blockchains are Proof-of-Work (PoW), Proof-of-Stake (PoS), Delegated Proof-of-Stake (DPoS), Practical Byzantine Fault Tolerance (PBFT), and RAFT [8]. These algorithms' employability might vary in terms of the byzantine fault tolerance, crash fault tolerance, speed of its verification, throughput of the transactions, and scalability.

One of the primary benefits of using blockchain is the ability to generate smart contracts such as Ethereum that currently uses Proof-of-Work (PoW) consensus protocol, NXT Proof-of-Stake (PoS), and Hyperledger Fabric Practical Byzantine Fault Tolerance (PBFT)[9]. According to [10], a smart contract converts a contract to computer codes, which are then stored and repeated on the computer system and monitored by the network of computers that operate the blockchain. A smart contract is a trusted application in automating the agreement execution, workflow and triggering the next action based on the policies and requirements specified in the contract and as agreed upon by the parties. The transactions are carried out in compliance with the terms of the contract [10] without any intermediary's involvement. As a result, transaction time and costs can be minimized because of smart contracts' ability to conduct themselves. Smart contracts not only describe the rules and penalties surrounding a contractual arrangement in the same way as conventional contracts do, but they also automatically impose those requirements. Smart contracts are self-verifying and self-executing agreements that can simplify the contract lifecycle to enhance enforcement, reduce risk, and increase business efficiencies [11]. Smart contracts have the benefit of efficiency and accuracy as they are digital and automated; security, trust, and transparency of the encrypted records of the transactions. There have been many applications of smart contracts across the industries which include supply chain areas to streamline and automate processes to identify any discrepancies, reconcile documents and transactions and resolve disputes based on the agreed-upon smart contract.

In this paper, a review of blockchain applications is presented in section 2. Section 3 presents the adoption of blockchain in supply chain sectors, and a discussion about the challenges faced in adopting blockchain is in section 4. Furthermore, some of the security issues are mentioned in section 5.

2. Blockchain Technology Applications

The blockchain technological concept became highly known after the first cryptocurrency, Bitcoin was introduced by Satoshi Nakamoto [12]. Nakamoto defined Bitcoin as a peer-to-peer version of electronic cash that allows online transactions to be sent directly without going through a centralized financial institution. The wide popularity of Bitcoin encouraged others to introduce their digital coins. But the concept of blockchain holds huge potential for large-scale improvements in different fields [13].

In blockchain, transactions are conducted in a multi-distributed form which can be used to transform and classify details. This is one of the applications of blockchain technology, in which all documents are stored securely and made available worldwide, with the ability to be verified at any time [14]. The variety of blockchain publications enriches various industries, including healthcare, banking, energy, media, and telecommunications. For example, the healthcare sector can use the features of blockchain to optimise data protection and authentication schemes for electronic health records.
The potential of blockchain technology to monitor transactions on distributed ledgers opens up new avenues for governments to increase accountability, prevent fraud, and foster confidence in the public-private sector. Some of the potential benefits such as trust and transparency can be especially beneficial for developing countries since they are more vulnerable to corruption, fraud, and lack of trust than developed countries [15]. Society can reduce the number of officials who execute regulations and provide administrative services and those officials who control this process (decreasing corruption, decreasing cost of public administration, increasing quality of administrative services). Another specific feature of the blockchain is an immutable repository. Therefore, the main idea is to use it as a general repository for any kind of public information which conventionally is managed by governments in the form of public registries, and administrative services around such registries, i.e. business registries, notaries, real estate and cadastral, public finances, trademarks and patents, and many others; which

makes an exhaustive list difficult. In general, we can say that the ledger can secure and timestamp any kind of facts [16].
Smart property refers to managing the responsibility of property or resources through the use of blockchain and smart contracts. The property can be tangible, such as an automobile, a home, or a cell phone or it can be non-physical, such as an organization's offers. Blockchain can envision placing proof of the existence of any authoritative archive, health records, and steadfastness instalments in the music industry, public accountants, private shares, and marriage licenses. The ambiguity or security goal can be achieved by keeping the unique mark of the computerized resource rather than the computerized resource itself.

3. Blockchain for Sustainable Supply Chain

Integrating IoT with blockchain enables the benefits of both technologies to form the decentralized model of blockchain that can handle processing of billions of transactions in between IoT devices. This can significantly reduce the costs associated with installing and maintaining large centralized data centers, distributing computation and storage of the devices that form the IoT networks [17].

As a result of its capability of ensuring public accessibility of data streams and data immutability, Blockchain can increase the transparency, efficiency, and reliability of the supply chains, and optimize the inbound processes. Many researchers are working on blockchain in logistics and supply chain activities as well. Radio-frequency identification (RFID), barcode, telematics, sensors-enabled technologies, Internet-of-things (IoT) and many other technologies are used for tracking products through the supply chain. [13]

Supply chains consist of a series of organisations and activities that products move through on their journey from the suppliers to the customers. The main goal for the organisations is to actively and collaboratively manage the operations in the supply chain to achieve a sustainable competitive advantage and maximize customer value [13]. Figure (1) presents the blockchain for Halal food supply chain.

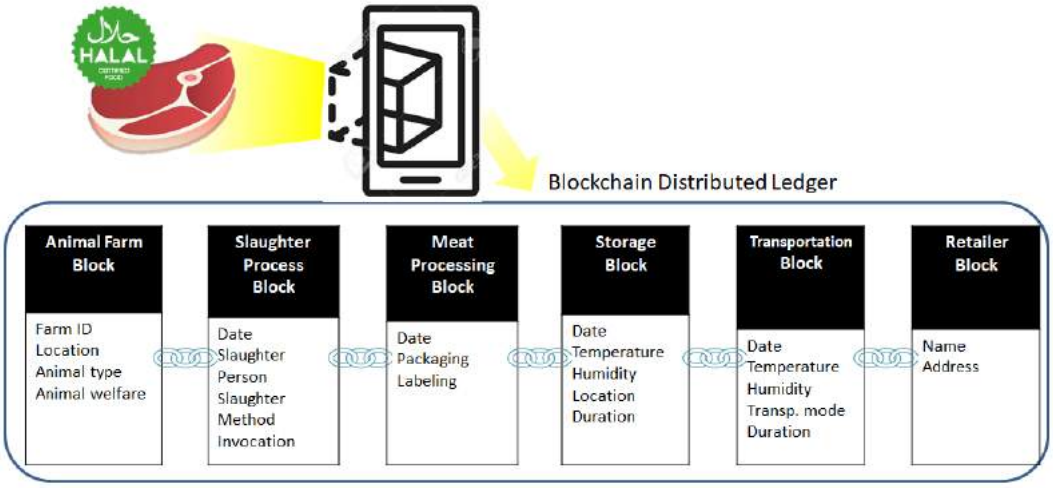

Fig1. Blockchain for Halal food supply chain

The studies about applications of blockchain in supply chain management are focusing on different aspects: First, tracing of assets as well as automation of supply chain operations, supply chain finance can be supported occasionally. Second, blockchain can reorganize supply chains for more collaborative ecosystems, such as: the security of additive manufacturing, agricultural supply chain, purchasing and supply management, common-pool resource management, and supply chain performance measurements [18]. Third, blockchain is subject to technical

limitations which are related to supply chain nature like: typically low data quality in supply chain settings and the governance model of data ownership [19].

A supply chain frequently crosses business functions and national borders, and it has a large network of trading partners. These interactions make the supply chain more vulnerable and can contribute to its disruption. Nowadays, supply chains are having three challenges: Data visibility, process optimization, and demand management. Many efforts were made to overcome them but the inefficiencies remain. An example of that is the administrative costs which are twice the cost of physically shipping the container [20].
Blockchain can play an important role in the area of supply chain by preventing security breaches and improving supply chain communication. Blockchain also provides automatic traceability, as append-only distributed databases of transaction information can be exchanged through the entire Peer-to-Peer network, and those historical records remain with permanent footprints in perpetuity. Besides that, a blockchain made up of nodes and arcs may be embedded in a traditional supply chain structure made up of nodes and arcs, allowing it to capture both operational and network risks associated with the supply chain [11].
Kehoe [21] summarized the main weaknesses of current supply chains and identified the four key solutions which can be provided by blockchain technology as shown in figure 2.

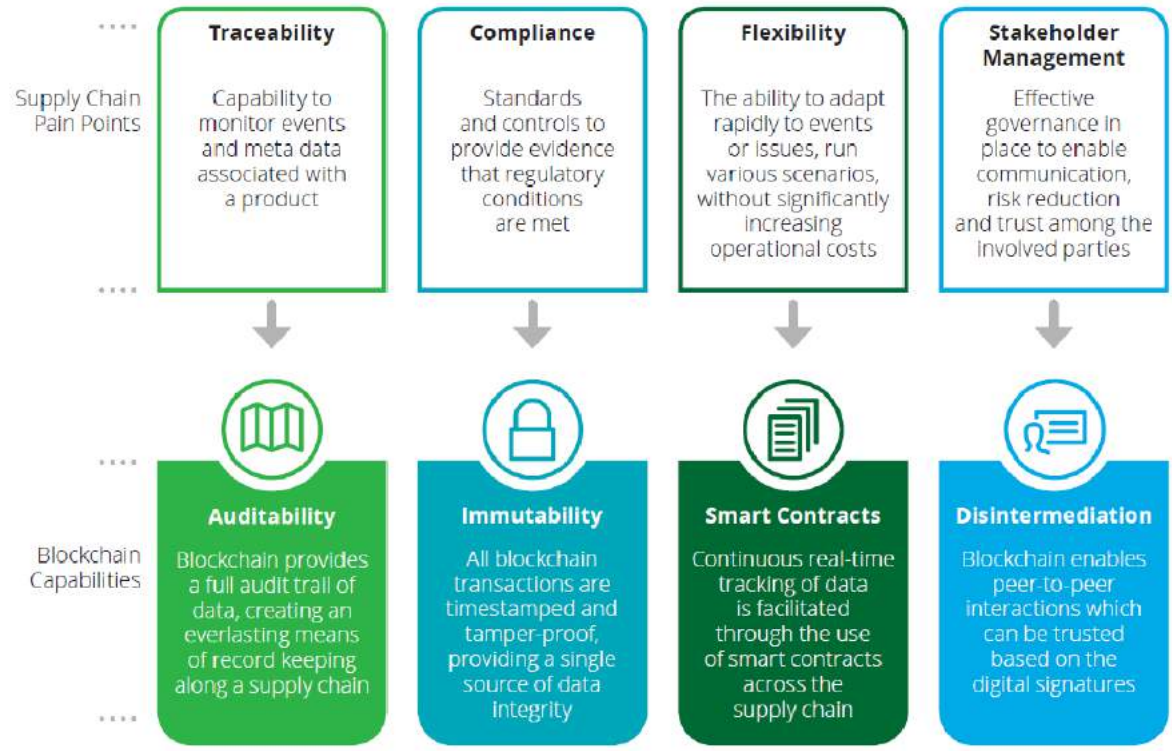

Fig 2. The four pain points in current supply chain and the blockchain possible solutions [21]

4. Blockchain Challenges in Supply Chain

With the amount of benefits and successes blockchain has achieved in various sectors, there are many shortcomings and vulnerabilities which are mainly due to its revolutionary concept and its complexity. Interoperability, scalability, and government regulatory concerns appear to be the most critical of these challenges. Since each node in a blockchain must process and verify each transaction, the blockchain needs a high-bandwidth internet connection, and massive processing power. If the blockchain is forced to centralize its verification process as a result of this obstacle, it will lose its original intent [11].

Furthermore, considering the various systems that blockchain technology can employ, determining the best combinations of platforms that are interoperable and compatible with one another will be difficult. Because blockchain is based on a distributed ledger that can escape government intervention, the government could put more pressure on blockchain users through various regulations and legal restrictions, reducing the utility of blockchain in terms of maintaining the integrity and privacy of transactions and asset transfers. Ironically, increased privacy makes it more difficult for law enforcement officials to determine who owns a digital wallet, making it more vulnerable to scammers attempting to steal digital currencies recorded on the blockchain [22].

Some of the major problems facing blockchain are summarized by [23]. Firstly, there is a lack of terminology clarification and perceived immaturity of the technology. There appears to be a lack of understanding among businesses, consumers and authorities about how the technology operates, the potential use cases for blockchain and the likely short and medium-term market development potential [24]. Secondly, there is insufficient data on the benefits to different kinds of businesses and the broader economic effects. Thirdly, the uncertainty of the regulatory environment, the multiple non-interoperable applications, as well as the fragmentation that occurs makes businesses avoid the adaptation of the technology[25]. Fourthly, technology has an energy-intensive nature. Also, the current supply chain models lack trust and certification for the products' path and the lack of trust regarding the compliance of the product with respect to origin, quality and specifications [11]. Typically, there are numerous supply chain members each with their own information systems, but communication between these systems is limited at best. [13] The interconnected structure of the supply chain makes it difficult to introduce a centralized system in control of a third party, since a high level of trust is required. The limited amount of trust concludes in separate systems that restrain the possibility to accomplish traceability throughout the full supply chain. [26].

5. Security Challenges of Blockchain

Numerous security experts believe that the blockchain system's intrinsic cryptographic existence is adequate to withstand persistent hacking and security threats. The adoption of blockchain technology in various sectors can help in improving the availability of unencrypted data as blockchain adopts a decentralized architecture, immutable reliable trust with verifiable transmission backtracks, secured transactions with cryptographic encryption, and keys as the unique identifiers. However, despite the many advantages that blockchains offer, blockchains are also vulnerable to attacks and require different types of consensus mechanisms and models to validate the transactions of the blockchain network. This mainly depends on the consensus algorithm such as Proof-of-Work (PoW), Proof-of-Stake (PoS), Delegated Proof-of-Stake (DPoS), Practical Byzantine Fault Tolerance (PBFT), and RAFT and their relative considerations as they have their characteristics. These consensus algorithms were analyzed in terms of their limitations, especially in the hashing power concentration where they are prone to attacks [27][6].

Among blockchain technology's problems are reversible transactions, verification speed, access restriction, cryptanalysis, anonymity, data mining, and modeling security [28]. Blockchain ensures security by doing a huge amount of repetition as the data have to be tampered proof. Nevertheless, it is possible that some of the nodes may act maliciously or can be compromised through the smart contract that runs on blockchain. Thus, it is important to ensure that any security vulnerabilities from other smart contracts do not get inherited when they are called [29].

Some of the blockchain security attacks are the Blockchain denial-of-service (BDoS) [30], endpoint security attacks, code vulnerabilities, malware mining, Sybil attacks [31], eclipse attacks [32], and routing attacks [29]. Other types of blockchain attacks are double-spending, privacy leakage, private key security, mining, and balanced attack [5]. Many approaches which include new consensus algorithms were made to deal with different aspects of security, privacy, and trust in the blockchain [33][34][35][36] in addition to other types of limitations such as the need for a trusted third party to act as a manager, the inability to reveal the identity of the signer in the event of a dispute, unresolved issue of the issuance and revocation of attribute certificate in a distributed environment, or the risk of data being deceived by a malicious user [28][35][36].

6. Conclusion

Blockchain offers numerous security characteristics that can increase the efficiency, and reliability of the supply chains, and optimize the inbound processes. It is also transparent and fault tolerant, in addition to its auditability, integrity, authorization, and privacy aspects. Blockchain also provides automatic traceability, as append-only distributed databases of transaction information can be exchanged through the entire network, and those records remain with permanent footprints. These characteristics are important in the supply chain area as it is difficult to centralize a system within the supply chain interconnected structure without a high level of trust within all the separate systems. This might restrain the possibility of full supply chain traceability. With the use of smart contracts that run on blockchain in the area of the supply chain, it is possible to quickly verify the location, history, and status processes that are accessible by anyone. Smart contracts automate the execution of agreements and other processes that can simplify the contract lifecycle to enhance enforcement, reduce risk, and increase business efficiencies. Blockchain can play an important role in the area of the supply chain as it helps in preventing security breaches and improving supply chain communication.

7. Acknowledgement

This research is supported by the Ministry of Higher Education (MoHE) of Malaysia through Fundamental Research Grant Scheme (FRGS/1/2020/ICT11/UUM/02/1).

REFERENCES

1. Khan, F. A., Asif, M., Ahmad, A., Alharbi, M., & Aljuaid, H. (2020). Blockchain technology, improvement suggestions, security challenges on smart grid and its application in healthcare for sustainable development. Sustainable Cities and Society, 55, 102018.
2. Picone, Marco; Cirani, Simone; Veltri, Luca (2021) "Blockchain Security and Privacy for the Internet of Things" Sensors 21, no. 3: 892. https://doi.org/10.3390/s21030892
3. Zheng, Z., Xie, S.,Dai, H-N., Chen, X. & Wang, H. (2018). Blockchain challenges and opportunities: a survey, International Journal of Web and Grid Services, 14(4), 352–375.
4. Nofer, M., Gomber, P., Hinz, O., & Schiereck, D. (2017). "Blockchain," Business & Information Systems Engineering, 59, 183-187
5. Mohanta, B. K., Jena, D., Panda, S. S., & Sobhanayak, S. (2019). Blockchain technology: A survey on applications and security privacy challenges. Internet of Things, 8, 100107.
6. Chaudhry, N., & Yousaf, M. M. (2018, December). Consensus algorithms in blockchain: Comparative analysis, challenges and opportunities. In 2018 12th International Conference on Open Source Systems and Technologies (ICOSST) (pp. 54-63). IEEE.
7. Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017, June). An overview of blockchain technology: Architecture, consensus, and future trends. In 2017 IEEE international congress on big data (BigData congress) (pp. 557-564). IEEE.
8. Khan, P.W.; Byun, Y.C.; Park, N. (2020) A Data Verification System for CCTV Surveillance Cameras Using Blockchain Technology in Smart Cities. Electronics, 9, 484.
9. Sankar, L. S., Sindhu, M., & Sethumadhavan, M. (2017, January). Survey of consensus protocols on blockchain applications. In 2017 4th International Conference on Advanced Computing and Communication Systems (ICACCS) (pp. 1-5). IEEE.
10. White, G. R. (2017). Future applications of blockchain in business and management: A Delphi study. Strategic Change, 26(5), 439-451.
11. Min, H. (2019). Blockchain technology for enhancing supply chain resilience. Business Horizons, 62(1), 35-45.
12. Nakamoto, S. (2008) Bitcoin: A Peer-to-Peer Electronic Cash System. https://bitcoin.org/bitcoin.pdf

13. Davor Dujak and Domagoj Sajter (2019) Blockchain Applications in Supply Chain. SMART Supply Network, EcoProduction, pp. 21-46 https://doi.org/10.1007/978-3-319-91668-2_2
14. Zyskind, G., & Nathan, O. (2015, May). Decentralizing privacy: Using blockchain to protect personal data. In 2015 IEEE Security and Privacy Workshops (pp. 180-184). IEEE.
15. Batubara, F. R., Ubacht, J., & Janssen, M. (2018, May). Challenges of blockchain technology adoption for e-government: a systematic literature review. In Proceedings of the 19th Annual International Conference on Digital Government Research: Governance in the Data Age (pp. 1-9).
16. Konashevych, O. (2017, June). The concept of the blockchain-based governing: Current issues and general vision. In The Proceedings of 17th European Conference on Digital Government ECDG (p. 79).
17. Atlam, Hany F., Alenezi, Ahmed, Alassafi, Madini O. and Wills, Gary (2018) Blockchain with Internet of Things: benefits, challenges, and future directions. International Journal of Intelligent Systems and Applications, 10 (6), 40-48, [2030]. (doi:10.5815/ijisa.2018.06.05).
18. YounessTribis, Abdelali El Bouchti, Houssine Bouayad (2018) Supply Chain Management based on Blockchain: A Systematic Mapping Study. MATEC Web of Conferences.
19. Blossey, G., Eisenhardt, J., and Hahn, G.2019. " Blockchain Technology in Supply Chain Management: An Application Perspective." In Proceedings of the 52nd Hawaii International Conference on System Sciences, edited by Tung Bui.
20. Shantanu Godbole (2017) How Blockchain can transform Global Trade Supply Chains. IBM Research, IBM Academy of Technology
21. Kehoe, L., & Ginder, K. (2017) When two chains combine: supply chain meets blockchain. Academic Press.
22. Hackett, R. (2017). Blockchain mania. Fortune, 178(3), 44—59.
23. Deshpande, A., Stewart, K., Lepetit, L., & Gunashekar, S. (2017). Distributed Ledger Technologies/Blockchain: Challenges, opportunities and the prospects for standards. Overview report The British Standards Institution (BSI), 40, 40.
24. Brandman & Thampapillai, 2016; Deloitte, 2016; Euro Banking Association Working Group on Electronic Alternative Payments (EBAWGEAP), 2016; McKinsey & Company.
25. Perboli, G., Musso, S., & Rosano, M. (2018). Blockchain in Logistics and Supply Chain: a Lean approach for designing real-world use cases. IEEE Access, 1–1. doi:10.1109/access.2018.2875782
26. Mahmood, B. B., Muazzam, M., Mumtaz, N., & Shah, S. H. (2019). A Technical Review on Blockchain Technologies: Applications, Security Issues & Challenges. International Journal of Computing and Communication Networks, 1(1), 26-34
27. Mingxiao, D., Xiaofeng, M., Zhe, Z., Xiangwei, W., & Qijun, C. (2017, October). A review on consensus algorithm of blockchain. In 2017 IEEE international conference on systems, man, and cybernetics (SMC) (pp. 2567-2572). IEEE.
28. Xiaoqi Li, Peng Jiang, Ting Chen, Xiapu Luo, and Qiaoyan Wen. (2017). A survey on the security of blockchain systems. Future Generation Computer Systems.
29. Azana Hafizah Mohd Aman, Wan Haslina Hassan, Shilan Sameen, Zainab Senan Attarbashi, Mojtaba Alizadeh, Liza Abdul Latiff (2021) IoMT amid COVID-19 pandemic: Application, architecture, technology, and security, Journal of Network and Computer Applications, Volume 174, 2021, 102886, ISSN 1084-8045.
30. Michael Mirkin, Yan Ji, Jonathan Pang, Ariah Klages-Mundt, Ittay Eyal, Ari Juels (2019) BDoS: Blockchain Denial of Service. arXiv:1912.07497
31. John R Douceur. 2002. The sybil attack. In International workshop on peer-to-peer systems. Springer, 251–260
32. Ethan Heilman, Alison Kendler, Aviv Zohar, and Sharon Goldberg. 2015. Eclipse attacks on bitcoin's peer-to-peer network. In 24th {USENIX} Security Symposium ({USENIX} Security 15). 129–144
33. K. Kesavarapu and V. Venkatesan (2019) Security Attacks on Blockchain, International Journal of Computer Applications (0975 –8887) Volume 178 – No. 16, pages 25-28
34. Litke, A., Anagnostopoulos, D., & Varvarigou, T. (2019). Blockchains for Supply Chain Management: Architectural Elements and Challenges Towards a Global Scale Deployment. Logistics, 3(1), 5. doi:10.3390/logistics3010005

35. Chang, Y., Iakovou, E., & Shi, W. (2019). Blockchain in global supply chains and cross border trade: a critical synthesis of the state-of-the-art, challenges and opportunities. International Journal of Production Research, 1–18. doi:10.1080/00207543.2019.1651946
36. Zhang, R., Xue, R., & Liu, L. (2019). Security and Privacy on Blockchain. ACM Computing Surveys, 52(3), 1–34. doi:10.1145/3316481