

Blockchain-IoT supply chain: systematic literature review

Umi Nabilah Badrol Said¹, Mohd Rizuan Baharon¹, Mohd Zaki Mas'ud¹, Ariff Idris¹, Noor Azurati Ahmad Salleh²

¹Department of Computer System and Communication, Faculty of Information and Communication Technology, Universiti Teknikal Malaysia Melaka, Melaka, Malaysia

²Faculty of Technology and Informatics Razak, Universiti Teknologi Malaysia, Johor, Malaysia

Article Info

Article history:

Received Oct 18, 2022

Revised Apr 07, 2023

Accepted Apr 30, 2023

Keywords:

Authentication

Blockchain

IoT

Supply chain

ABSTRACT

Since 2016, the implementation of blockchain in the supply chain has attracted wide interest among researchers. The creation and study of blockchain technology have grown at an exponential rate in the last decade. The supply chain would be a massive technological leap with the combination of blockchain technology that brings major changes to different facets of the industry, such as record immutability, improved traceability, quality assurance, improved knowledge flows, decentralized power structure, and decreased chances of fraud. With the growth in blockchain Internet-of-Thing (IoT) supply chain technologies, the security risk of implementing such technologies and methods to counter it has been largely discussed among researchers. This study analyses peer-reviewed literature attempting to use authentication in the blockchain-IoT supply chain to counter security risks in the technologies and provides a comprehensive analysis of the important feature when creating an authentication technique for the blockchain-IoT supply chain. Finally, the study discusses some of the problems and research objectives in the realm of authentication in the blockchain-IoT supply chain.

This is an open-access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.



Corresponding Author:

Mohd Rizuan Baharon

Department of Computer System and Communication

Faculty of Information and Communication Technology, Universiti Teknikal Malaysia Melaka

76100, Melaka, Malaysia

Email: mohd.rizuan@utem.edu.my

1. INTRODUCTION

Blockchain Internet-of-Thing (IoT) supply chain is one of the latest integrations of blockchain and IoT technology which aims to enhance traceability and transparency of the supply chain. On the one hand, blockchain technology supports decentralized, trust-free, traceable, and smart contracts. On the other hand, the IoT helps to connect multiple devices and sensors. The integration of both IoT and blockchain technology produces a huge amount of data. Such integration has brought an efficient and money-saving solution [1]. Unfortunately, the blockchain-IoT supply chain is used by a small percentage of food and beverage industry manufacturers [2], [3]. The reason is that the supply chain involves a lot of individual and entities, from mere producer to consumers, most of the entities involved does not trust the security and privacy of data stored inside the blockchain-IoT supply chain. To increase the entities, trust in the system, various research was conducted to secure end-to-end transaction processes in the system. Most notably, there is an emerging trend in the concept of blockchain-IoT supply chain authentication. In this study, we seek answers to research questions and propose new paths by identifying and critically examining existing research specifically relevant to authentication technique use in protecting the blockchain-IoT supply chain.

There appears to be no systematic literature review (SLR) on the topic of authentication techniques utilized in blockchain-IoT supply chains, to the best of our knowledge. Astill *et al.* [4] recently published one of the most recent reviews of the IoT-enabling technology and the methodology that can be used to handle data in the food supply chain, including blockchain and big data analytics. However, blockchain also demands a significant portion of processing resources from network servers, which is a problem for both economic and environmental reasons. Furthermore, Lone and Naaz [5] have described the security of the internet and IoT can be achieved by using the blockchain smart contract. They explored how smart contracts improve internet and IoT security, as well as their limitations. At the end of 2018, Wang *et al.* [6] conduct an SLR that intends to look at how blockchain technology will affect supply chain practices and policies in the future. Their finding shows that there is an increase in the adoption of blockchain technologies, supply chain digitalization and disintermediation, extended visibility and traceability, stronger data security, and smart contracts are four areas where such technologies add value to supply chain management.

All the past work we considered answered questions about the usage of blockchain technology in a broader context. They do not, however, evaluate or research the authentication approach that can be used to secure the blockchain-IoT supply chain. This field is rapidly developing and has a lot of potential. As a result, to direct and encourage further research in this area, it is required to supply state-of-the-art literature or the most recent results from this research field. The purpose of this paper is to review existing research, compile findings, and summarize empirical data on the authentication technique used in the blockchain-IoT supply chain. This paper is conducted to achieve objectives, which are to identify the most common features to be considered for establishing a secure authentication technique in the blockchain-IoT supply chain. Furthermore, we aim to determine whether the authentication technique meets the IoT requirement to ensure the availability of the blockchain-IoT supply chain.

The rest of the paper is structured as follows. The methods used to systematically select the primary studies for analysis are described in section 2. The results of the analysis of all the primary studies chosen and their discussion are presented in section 3. Section 4 provides a conclusion and future research directions in authentication mechanism configuration in the blockchain-IoT supply chain.

2. METHOD

2.1. Selection of primary studies

In primary studies, keywords were entered into a search engine's file browser. Such keywords help to discover related research works that effectively address the research problem. AND and OR were the only Boolean operator used. The search strings were: "Authentication" AND ("block-chain" OR "blockchain" OR "distributed ledger") AND "supply chain" AND ("Internet of Thing" OR "IoT" OR "Internet-of-Thing") The platforms searched were ScienceDirect, Google Scholar, Research Gate and IEEE Xplore Digital Library.

2.2. Criteria for inclusion and exclusion

New technological blockchain implementations, case studies, and commentaries on the progress of existing blockchain adoption in both supply chain and IoT are examples of studies that would be included in this SLR. The paper must be written in English and peer-reviewed. Since Google Scholar can produce lower-quality papers, any Google Scholar results will be checked for compliance with these criteria. Thus, this SLR only covers the most recent edition of the study and the main criteria for inclusion and exclusion are listed in Table 1.

Table 1. Primary studies criteria for inclusion and exclusion

| Inclusion criteria | Exclusion criteria |
|--|---|
| <ul style="list-style-type: none"> - The study must contain empirical details about the authentication technique used in the IoT-blockchain technology. - Details about blockchain or applicable distributed ledger technology must be included in the study. - It must be a peer-reviewed study that has been published in the proceedings of a conference or a journal. | <ul style="list-style-type: none"> - Study that discusses blockchain technology's economic, industrial, and legal implications. - Any grey literature, for example, government reports, statistics, and patents. - Articles published in languages other than English. |

2.3. Result selection

As shown in Figure 1, the preliminary keyword searches on the selected pages yielded a total of 217 studies. After duplicate studies were withdrawn, the number was reduced to 167. There were 58 papers left to read after reviewing the studies against the inclusion/exclusion criterion. After reading all 58 papers in their entirety and re-applying to the inclusion/exclusion criteria, 38 papers remained. Snowballing forward and backward showed another 1 and 1 posts, taking the total number of papers in this SLR to 40.

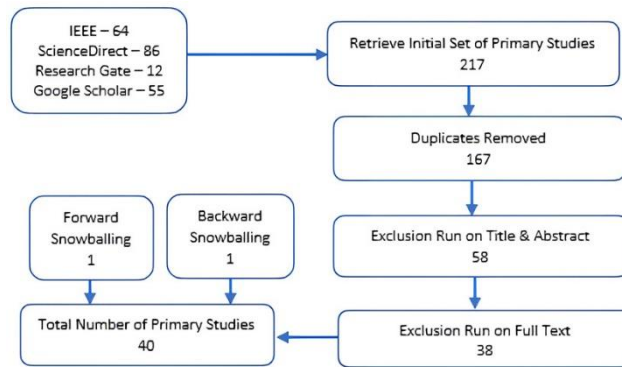


Figure 1. Extraction of paper through

2.4. Quality evaluation

Kitchenham and charters' guidelines for evaluating the consistency of primary studies were followed. This provided for an evaluation of the paper's relevance to the research issues, as well as any indicators of research inequity and the reliability of experimental results. The evaluation procedure was based on that of Hosseini *et al.* [7]. Ten papers were chosen randomly and confined to the following quality evaluation process to evaluate their efficacy. Afterward, the quality-control checklist was extended to all other primary chosen studies. As shown in Table 2, there are five studies excluded from the SLR since it studies failed to comply with a checklist.

Table 2. Excluded studies

| Criteria stages | Excluded studies |
|-------------------------------------|------------------|
| Level 1: authentication | [8] |
| Level 2: context | [9] |
| Level 3: authentication application | [9] |
| Level 4: authentication performance | [8], [9], [10] |
| Level 5: data acquisition | [10] |

2.5. Extraction of data

Data was collected from all papers that passed the quality evaluation to determine the validity of data and verify the correct documentation of information found within the papers. The data extraction approach was evaluated on ten studies first, then expanded to incorporate all studies that passed the quality evaluation process. Three categories were used to extract and categorize the data from each study which included context data, qualitative data, and quantitative data.

2.6. Analysis of data

The data from the qualitative and quantitative data categories were collected to address the research questions. In addition, a meta-analysis of publications over time and the significant keyword used is conducted to identify the development of the research paper and topic of interest of all the final studies chosen.

a) Publication over time

After Satoshi Nakamura's concept of blockchain was published in 2008, it was not until 2016 that the first primary research papers on supply chain integration in the blockchain were published. Since then, the security of IoT device implemented in the scheme have gained the interest of researcher and a few papers regarding robust authentication method to secure IoT devices has been has been written. The Figure 2 depicting the number of primary studies conducted per year. As seen in the graph, there is an exponential increase in the suggested authentication method for securing the IoT-blockchain supply chain. As the number of publications continues to grow year after year, and this study is only up to July 2021, expect a significant number of scientific studies on the authentication method used to secure blockchain-IoT supply chain in the future.

b) Significant keywords in primary studies

A keyword search was performed through all 37 studies to outline the recurrent characteristics among the selected primary studies. Table 3 shows how many times each word was used in each primary study. Except for the keywords selected by the author, namely "authentication," "blockchain," "supply chain," and "IoT," the keyword commonly found in the dataset, is "security," as shown in the table. This demonstrates that the use of blockchain technology in the sense of the IoT supply chain has resulted in a few security issues that may affect confidentiality, integrity, and availability of data acquisition; this will be discussed further in section 3.

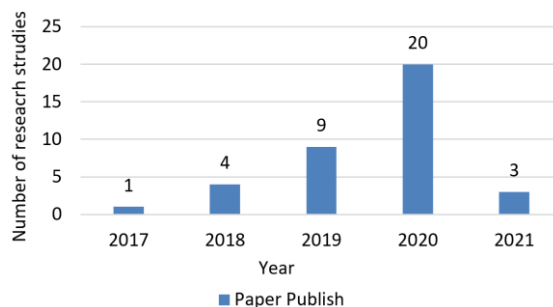


Figure 2. Primary studies published over time

Table 3. Total keywords count in primary studies

| Keyword | Count | Keyword | Count |
|----------------|-------|----------------|-------|
| Blockchain | 1682 | Smart contract | 610 |
| Authentication | 1364 | Sensor | 498 |
| Security | 1286 | Traceability | 394 |
| Supply chain | 1074 | Transparency | 196 |
| IoT | 1019 | Scalability | 174 |
| Node | 929 | Tracking | 173 |

3. RESULTS AND DISCUSSION

3.1. Results

Table 4 summarizes the qualitative and quantitative data obtained from them. The key findings are divided into two categories; key finding and authentication algorithm. The key finding that focuses on the subject or theme of all the primary studies was the authentication process that was implemented on the blockchain-IoT supply chain. All this data is grouped into a chart figure, a detailed explanation of the charts is further examined in the n discussion section. Figure 3 presents the authentication algorithm or technique to secure the interaction and data travel in the blockchain-IoT supply chain. Figure 4 shows the percentages of challenges and the open issue of the primary studies identified by the SLR.

3.2. Discussion

Initial keyword searches reveal a sizable number of articles that are related to blockchain. Blockchain innovation and fully distributed autonomous networks are still in their early stages since their existence of nearly thirteen years. In addition, most of the selected primary studies are focused on theories or ideas to answer current problems, with no objective evidence and few practical implementations. The remaining primary studies demonstrate a few of the more functional and secure applications, and they demonstrate innovative strategies for solving different areas of problems, including mutability, user authentication, and data security. The applications oftentimes necessitate a significant shift in the system's architecture, such as a different network design or platform or a specific blockchain used rather than the use of the centralized server.

a) RQ1: what are the features which can be considered in a process of authentication and validation?

Authentication is the process of identifying users that request access to a system, network, or device. Going through the primary studies, we highlighted features that the study is using to create their authentication technique. From Figure 4, cost relates to storage, communication, computational, effectiveness, security of the product, and security of the network is the main features addressed to create an effective and secure authentication technique. Applying authentication on a resource-constrained IoT device is a challenge that most of the latest primary studies trying to tackle to provide scalability and availability to the system [11]–[23]. Higher throughput and low latency while providing security are the aims of this primary study, therefore, they focus on the storage, communication, and computational cost of the authentication technique. Then, the gas unit is used to measure the cost-effectiveness of the transaction, which is based on the transaction's complexity. While the latest study focuses on the resource constraint aspect of an IoT device, the leadoff study [15], [24]–[29], focuses more on the security of the product. The authentication technique solely depends on the infrastructure of the blockchain, without considering the effect of using traditional authentication techniques on an IoT device. The feature that this study trying to protect is the system data privacy, integrity and transparency [16], [28], [30]–[32]. Soon after, the security of the network become the focus of the authentication technique, this is because, even though blockchain is deemed to be immutability, it still faces security threats from an adversary that wanted access to the system via exploitation of IoT weakness.

b) RQ2: what is the authentication algorithm to validate the legitimate and fraudulent nodes?

The existing blockchain – IoT supply chain security solutions rely mostly on a single trusted central authority, making them vulnerable to assaults varying from a single point of failure to denial of service. Based on the features identified in the RQ1, most of the latest primary studies chosen have aimed to improve the protection and reliability of the system via a robust authentication technique. Figure 3 shows the type of authentication and encryption technique identified from the primary studies. Access control list and peer-to-peer authentication is the most commence authentication technique suggested, they fit the decentralized aspect of blockchain technologies and it benefit out of smart contract. However, access control lists implemented by smart contracts may have issues due to their non-upgradable character, i.e., their inability to respond to development changes such as fixing a vulnerability in a smart contract that has already been deployed. While the decentralized component of blockchain appears to promote peer-to-peer authentication, each request for authentication or access blockchain grows, and each transaction has a storage cost, this could limit their scalability in fulfilling the demands of some IoT applications. To combat this, some papers suggested changes in the encryption technique used. Public key infrastructure (PKI) is one of the most used encryption techniques in primary studies, followed by the hash function, elliptic curve cryptography (ECC), and Rivest-Shamir-Adleman cryptography (RSA). This encryption technique is used to generate keys during the authentication process, the hash function was used to encrypt the data traveling inside the blockchain. Then some papers suggested unique encryption techniques that claim to be more secure and less complex than the standard PKI [17], [18], [20], [32], [33]. With millions of IoT devices connected to the internet, some of these unique encryption approaches still have security issues, making it difficult to fulfill the high transaction throughput and low latency requirements of IoT. Lastly, there was also a paper that suggested the use of biometric authentication [19], [31] in blockchain. However, this feature can be a hindrance to IoT devices due to the consumption of space needed to store this information.

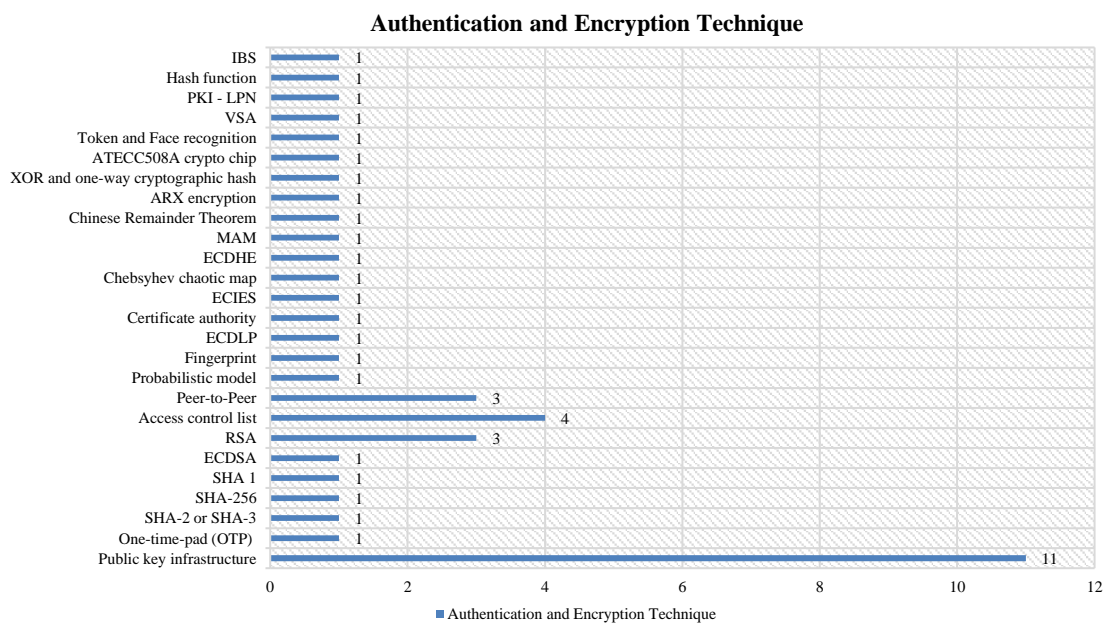


Figure 3. The authentication method used in primary studies

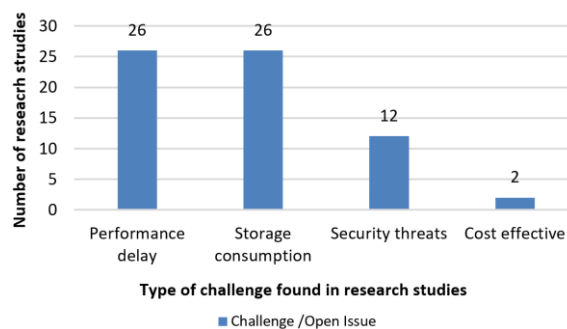


Figure 4. Challenges and open issues identified in primary studies

Table 4. Themes and key findings of primary studies

| Primary study | Key findings | Authentication algorithm |
|---------------|---|--|
| [11] | Proposes a protected blockchain-enabled supply chain management system that combines a decentralized database (permission blockchain) and a flexible ultra-lightweight shared authentication radio frequency identification (RFID) protocol. Challenges/issues: secret disclosure attack, replay attack, a man-in-the-middle attack, traceability attack, storage cost, communication cost, computational cost de-synchronization attack. | Secure Hash Algorithm 256 (SHA-256) and access control list |
| [23] | Creates an IoT-oriented permissioned blockchain that includes a novel sharding method for unstable distributed networks called distributed ledger for IoT data (DLIT), which is covered by a scalable distributed ledger (DL). Challenges/issues: storage cost, communication cost, computational cost. | RSA |
| [13] | In the IaaS cloud, a blockchain architecture for provenance preservation and evidence collection is built. Challenges/issues: non-repudiation, storage cost, communication cost, computational cost. | Elliptic curve integrated encryption scheme |
| [14] | A smart contract is used to offer the framework for securely distributing specified cryptographic keys to all participants. Challenges/issues: man-in-the-middle attack, replay attack, communication cost, computational cost. | Validator selection algorithm and public key infrastructure |
| [15] | Consist of organizational level demonstrates the relationship between supply chain partners and related network architecture and the operational level demonstrates smart contracts and transaction validation standards. Challenges/issues: security of the product, storage cost, communication cost, computational cost. | RSA |
| [12] | Is a lightweight consensus blockchain architecture (LC4IoT) that forms a supply chain with various distributed IoT devices. Challenges/issues: storage cost, communication cost, computational cost. | Public key infrastructure |
| [16] | Introduces the notion of ring signatures and provides reliable data exchange over the network and cloud storage. Challenges/issues: data privacy, intruder attack, storage cost, communication cost. | Addition, Rotation, Exclusive – OR (ARX) encryption |
| [17] | A lightweight authentication and authorization system to ensure the safety and integrity of data in the Blockchain-enabled IoT network is being developed. Applications and networks are the two components that make up the framework. Challenges/issues: impersonation, man-in-the-middle attack, dos attack, replay attack, timing attack, forgery, storage cost, communication cost, computational cost. | Probabilistic model |
| [18] | The implementation of a secure, portable, and platform-agnostic blockchain tokenizer for industrial IoT trustless applications is described in this study. Challenges/issues: cost-effective, storage cost, communication cost, computational cost. | ATECC508A crypto chip |
| [19] | CAB-IoT allows continuous authentication for the IoT environment that is real-time and non-intrusive. It uses a trust module to detect outliers and irregular access that are based on a face recognition machine learning model. Challenges/issues: man-in-the-middle attack, replay attack, DoS and DDoS attack, Sybil attack, storage cost, non-repudiation, communication cost, computational cost. | Token and face recognition |
| [20] | Suggest privacy-preserving user authentication based on a secret computational model of a physically unclonable function (PUF) and blockchain technology. Challenges/issues: DoS and DDoS attack, replay attack, man-in-the-middle attack, storage cost, impersonation, communication cost, computational cost. | Chinese remainder theorem and Hash function |
| [21] | An alternate authentication strategy is presented in this study, in which it produces a secret key internally, utilizing manufacturing variation as a physical unclonable function (PUF). Challenges/issues: storage cost, communication cost, computational cost. | Public-key cryptography based on learning parity with noise (LPN) problems, and zero-knowledge Certificate authority |
| [22] | Proof of block & trade (PoBT) consensus algorithm for IoT blockchain reduced computation time by allowing the validation of trades and the blocks. Challenges/issues: 51% attack, storage cost, communication cost, computational cost. | |
| [24] | This study introduces the use of a proof-of-work (PoW) consensus algorithm with BigchainDB, to create a highly scalable decentralized system. Challenges/issue: security of the product. | Public key infrastructure |
| [25] | A trusted trade blockchain network cloud platform is a food traceability system based on blockchain and IoT technologies that is reliable, self-organized, open, and environmentally sustainable, involving the stakeholders in a smart agriculture system. Challenges/issue: security of the product. | Peer-to-Peer |
| [26] | Present FARMer and Rely (FARMAR) a novel project for supply chain management in agriculture by embedding blockchain Technology (BigchainDB). Challenges/issue: security of the product. | Public key infrastructure |
| [27] | It is a permission system based on an Ethereum smart contract that allowed tracking and tracing of items. Challenges/issue: security of the product. | Access control list |
| [28] | The platform's goal is to give safe storage for huge volumes of agriculture data that cannot be compromised for fish farmers. Smart contracts were used to minimize the chance of error or coercion. Challenges/issues: data integrity, and security of the product. | Public key infrastructure |
| [29] | Propose a blockchain-based digital ledger for food products, providing user access to data regarding production, quality, market, and price. Challenges/issue: security of the product. | Public key infrastructure |

Table 4. Themes and key findings of the primary studies (*continue*)

| Primary study | Key findings | Authentication algorithm |
|---------------|--|--|
| [30] | Using blockchain technology to improve supply chain transparency for both manufacturers and customers, as well as legal supply chain coordination. Challenges/issue: Data transparency. | Peer-to-peer |
| [31] | A scalable and secure IoT-enabled supply chain traceability, it keeps data and data fingerprints in off-chain storages and blockchain, it also has an agile transaction delivery ratio that may be used to track latency and cost in response to demand. Challenges/issues: data integrity, forgery. | Fingerprint |
| [32] | To discover operational disruptions or counterfeiting difficulties, a transparent product ledger based on trade event details and time-stamped supply chain procedures. It also takes advantage of Interest on trust account's masked authenticated message (IOTA's MAM) protocol. Challenges/issues: data integrity, non-repudiation. | N-th degree truncated polynomial ring units (NTRU) key exchange protocol and masked authentication messaging |
| [33] | Introduce two decentralized mutual authentication protocols for IoT systems that use closed-loop RFID systems (CLAB) and open-loop RFID systems (OLAB), respectively. Challenges/issues: impersonation, DoS attack, traceability attack, replay attack, de-synchronization attack, secret disclosure attack. | Chebyshev chaotic map |
| [34] | Propose a secure decentralized location-based device-to-device (D2D) authentication architecture in which fog devices can use blockchain to mutually authenticate each other at the fog layer. Challenges/issues: man-in-the-middle attack, replay attack, secret key guessing attack, data privacy, impersonation. | Peer-to-peer |
| [35] | Develop a blockchain that uses self-attestation and consensus among IoT devices to incrementally update a trusted anomaly detection model. Challenges/issues: buffer overflow, data poisoning attack, DoS, DDoS attack, replay attack. | Public key infrastructure |
| [36] | For a defense-in-depth method, a "locally permissioned" blockchain system is used to authenticate edge devices regularly to avoid cloning. Scribe used a lightweight mining algorithm to randomize the miner selection. Challenges/issues: illegitimate registration, replay attack, DoS attack, DDoS attack | One-time-pad (OTP) and SHA-2 or SHA-3 |
| [37] | A slim proxy software development kit (SDK) on the server is used to maintain complete control over the device's transactions by holding a standard blockchain identity with its private key. Challenges/issue: replay attack, dos attack. | Public key infrastructure |
| [38] | IBCbAP is an enhanced blockchain-based authentication protocol with security features like secure access control and anonymity. Challenges/issues: DDos attack, replay attack, traceability attack, secret disclosure attack. | Elliptic curve discrete logarithm problem and Hash-based message authentication code (HMAC) |
| [39] | A blockchain-based product traceability architecture for a cross-border e-commerce supply chain. It incorporates several blockchain-based models, such as the data management model, block structure model, and multi-chain structure model. Challenges/issues: impersonation, clone attack. | Elliptical encryption digital signature algorithm and RSA |
| [40] | Propose a three-tiered trust management system that employs a consortium blockchain to monitor supply chain interactions and dynamically assign trust and reputation values based on them. Challenges/issues: malicious peer attack, Sybil attack, ballot stuffing attack, whitewashing attack, non-repudiation, impersonation. | Public key infrastructure |
| [41] | Blockchain and IoT are being used to make the drug supply chain transparent to increase trust between actors and provide privacy, traceability, and authenticity. Challenges/issues: non-repudiation, forgery. | SHA – 1 |
| [42] | Implemented a low-cost blockchain-based system for tracking and tracing every chip as it circulates across the supply chain using consortium blockchain. Challenges/issues: illegitimate registration, illegitimate transfer. | Access control list |
| [43] | Suggest a shared, three-tiered architecture that guarantees data availability to customers, restricts access to competitors, and scales to handle transaction volume. They also suggest a transaction vocabulary as well as access rights for handling read and write privileges on the consortium's blockchain. Challenges/issue: ID spoofing attack, Sybil attack, 51% attack. | Access control list |
| [44] | Suggest a connection to facilitate the sharing of product and material tracking data across parties while preserving the parties' privacy using a private blockchain. Challenges/issue: Sybil attack, 51% attack. | Public key infrastructure |
| [45] | Privacy-preserving data processing in cloud computing. Challenges/issue: noise size in ciphertext data. | Lightweight encryption scheme |
| [46] | Present a 5-layered state-of-the-art secure and efficient framework for dealing with IoT-based blockchain protection and privacy issues. Challenges/issues: storage cost, communication cost, computational cost. | Public key infrastructure |
| [47] | Present a lightweight blockchain-enabled RFID-based authentication protocol (LBRAPS) for supply chains within a 5G environment of mobile edge computing. Challenges/issues: impersonation, data poisoning attack, man-in-the-middle attack, replay attack, ephemeral secret leakage attack, communication cost, computational cost. | XOR and one-way cryptographic hash |
| [48] | Suggests the use of several security gateways to create a centralized cloud-based cross-domain data exchange platform. The information is stored in the centralized cloud using the blockchain via the security gateways. Challenges/issues: storage cost, communication cost, computational cost. | Ephemeral elliptic curve Diffie-Hellman and identity-based Signature |

4. CONCLUSION

The emerging technology of blockchain and IoT contexts have brought many underlying concerns and challenges. In this section, we address some of the fundamental difficulties identified from the primary studies' security solutions. Our studies suggest that the authentication of nodes in the blockchain-IoT supply chain is important to reduce the security risk of an IoT device. Even though the authentication secures the channel for data transactions, the transparency by design and transaction pattern analysis aspect of the blockchain can cause unintentional occasional disclosures of data such as the identities of individuals or devices hiding behind public keys. We offer the following potential research directions for authentication in the blockchain-IoT supply chain for protecting the System in general and IoT in particular, based on the results of this SLR and our observations: the need for a robust and lightweight authentication technique to meet the requirement of IoT devices with limited resources in a highly scalable platform and the need for an encryption scheme that will cater the data privacy issue while maintaining transparency in a highly scalable platform.

ACKNOWLEDGEMENTS

The authors would like to extend their appreciation to the Ministry of Higher Education (MoHE) of Malaysia, Universiti Teknikal Malaysia Melaka (UTeM) and Universiti Teknologi Malaysia (UTM) for providing financial support for this study through the Collaborative Research Grant National PJP/2019/FTMK-CACT/CRG/S01709 (UTeM) and R.K130000.7314.4B581(UTM).




REFERENCES

- [1] A. H. Mohammed and R. M. A. Hussein, "A Security Services for Internet of Thing Smart Health Care Solutions Based Blockchain Technology," *Telecommunication, Computing, Electronics and Control (TELKOMNIKA)*, vol. 20, no. 4, pp. 772–779, 2022, doi: 10.12928/TELKOMNIKA.v20i4.23765.
- [2] A. Rejeb, "Blockchain Potential in Tilapia Supply Chain in Ghana," *Acta Technica Jaurinensis*, vol. 11, no. 2, pp. 104–118, 2018, doi: 10.14513/actatechjaur.v11.n2.462.
- [3] L. Sripathi, "Adoption of Blockchain technology in food supply chain management," *Creative Components*, no. 346, 2019. [Online]. Available: <https://core.ac.uk/download/pdf/232931128.pdf>
- [4] J. Astill *et al.*, "Transparency in food supply chains: A review of enabling technology solutions," *Trends in Food Science & Technology*, vol. 91, pp. 240–247, 2019, doi: 10.1016/j.tifs.2019.07.024.
- [5] A. H. Lone and R. Naaz, "Applicability of Blockchain smart contracts in securing Internet and IoT: A systematic literature review," *Computer Science Review*, vol. 39, 2021, doi: 10.1016/j.cosrev.2020.100360.
- [6] Y. Wang, J. H. Han, and P. B. -Davies, "Understanding blockchain technology for future supply chains: a systematic literature review and research agenda," *Journals Supply Chain Management*, vol. 24, no. 1, pp. 62–84, 2019, doi: 10.1108/SCM-03-2018-0148.
- [7] S. Hosseini, B. Turhan, and D. Gunarathna, "A Systematic Literature Review and Meta-Analysis on Cross Project Defect Prediction," in *IEEE Transactions on Software Engineering*, vol. 45, no. 2, pp. 111-147, 2019, doi: 10.1109/TSE.2017.2770124.
- [8] A. Abdullah, E. Stroulia, and F. Nawaz, "Efficiency Optimization in Supply Chain Using RFID Technology," *2020 IEEE Intl Conf on Dependable, Autonomic and Secure Computing, Intl Conf on Pervasive Intelligence and Computing, Intl Conf on Cloud and Big Data Computing, Intl Conf on Cyber Science and Technology Congress (DASC/PiCom/CBDCCom/CyberSciTech)*, 2020, pp. 1-6, doi: 10.1109/DASC-PiCom-CBDCCom-CyberSciTech49142.2020.00017.
- [9] A. S. Sangeetha, S. Shunmugan, and G. Murugan, "Blockchain for IoT Enabled Supply Chain Management - A Systematic Review," *2020 Fourth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)*, 2020, pp. 48-52, doi: 10.1109/I-SMAC49090.2020.9243371.
- [10] E. Mahan, "Seafood is off the Chain! How do we integrate Blockchain Technology for Seafood Traceability?," *Scripps Institution of Oceanography*, 2020. [Online]. Available: <https://escholarship.org/uc/item/4385m32n>
- [11] M. Sidorov, M. T. Ong, R. V. Sridharan, J. Nakamura, R. Ohmura, and J. H. Khor, "Ultralightweight Mutual Authentication RFID Protocol for Blockchain Enabled Supply Chains," in *IEEE Access*, vol. 7, pp. 7273-7285, 2019, doi: 10.1109/ACCESS.2018.2890389.
- [12] H. Moudoud, S. Cherkaoui, and L. Khokhi, "An IoT Blockchain Architecture Using Oracles and Smart Contracts: the Use-Case of a Food Supply Chain," *2019 IEEE 30th Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC)*, 2019, pp. 1-6, doi: 10.1109/PIMRC.2019.8904404.
- [13] P. Velmurugadass, S. Dhanasekaran, S. S. Anand, and V. Vasudevan, "Enhancing Blockchain security in cloud computing with IoT environment using ECIES and cryptography hash algorithm," *Materials Today: Proceedings*, 2021, vol. 37, pp. 2653–2659, doi: 10.1016/j.matpr.2020.08.519.
- [14] S. K. Dwivedi, R. Amin, and S. Vollala, "Blockchain based secured information sharing protocol in supply chain management system with key distribution mechanism," *Journal of Information Security and Applications*, vol. 54, 2020, doi: 10.1016/j.jisa.2020.102554.
- [15] T. K. Agrawal, V. Kumar, R. Pal, L. Wang, and Y. Chen, "Blockchain-based framework for supply chain traceability: A case example of textile and clothing industry," *Computers & Industrial Engineering*, vol. 154, 2021, doi: 10.1016/j.cie.2021.107130.
- [16] G. Srivastava, J. Crichigno, and S. Dhar, "A Light and Secure Healthcare Blockchain for IoT Medical Devices," *2019 IEEE Canadian Conference of Electrical and Computer Engineering (CCECE)*, 2019, pp. 1-5, doi: 10.1109/CCECE.2019.8861593.
- [17] M. Tahir, M. Sardaraz, S. Muhammad, and M. S. Khan, "A Lightweight Authentication and Authorization Framework for Blockchain-Enabled IoT Network in Health-Informatics," *Sustainability*, vol. 12, no. 17, 2020, doi: 10.3390/su12176960.
- [18] D. Mazzei *et al.*, "A Blockchain Tokenizer for Industrial IOT trustless applications," *Future Generation Computer Systems*, vol. 105, pp. 432–445, 2020, doi: 10.1016/j.future.2019.12.020.
- [19] F. H. Al-Naji and R. Zagrouba, "CAB-IoT: Continuous authentication architecture based on Blockchain for internet of things," *Journal of King Saud University - Computer and Information Sciences*, vol. 34, no. 6, pp. 2497-2514, 2022, doi: 10.1016/j.jksuci.2020.11.023.




- [20] A. S. Patil, R. Hamza, A. Hassan, N. Jiang, H. Yan, and J. Li, "Efficient privacy-preserving authentication protocol using PUFs with blockchain smart contracts," *Computers & Security*, vol. 97, 2020, doi: 10.1016/j.cose.2020.101958.
- [21] M. Á. P. -Delgado, I. Baturone, G. Dittmann, J. Jelitto, and A. Kind, "PUF-derived IoT identities in a zero-knowledge protocol for blockchain," *Internet of Things*, vol. 9, 2020, doi: 10.1016/j.iot.2019.100057.
- [22] S. Biswas, K. Sharif, F. Li, S. Maharjan, S. P. Mohanty, and Y. Wang, "PoBT: A Lightweight Consensus Algorithm for Scalable IoT Business Blockchain," in *IEEE Internet of Things Journal*, vol. 7, no. 3, pp. 2343-2355, 2020, doi: 10.1109/JIOT.2019.2958077.
- [23] S. R. Niya, R. Beckmann, and B. Stiller, "DLIT: A Scalable Distributed Ledger for IoT Data," *2020 Second International Conference on Blockchain Computing and Applications (BCCA)*, 2020, pp. 100-107, doi: 10.1109/BCCA50787.2020.9274456.
- [24] F. Tian, "A supply chain traceability system for food safety based on HACCP, blockchain & Internet of things," *2017 International Conference on Service Systems and Service Management*, 2017, pp. 1-6, doi: 10.1109/ICSSSM.2017.7996119.
- [25] J. Lin, Z. Shen, A. Zhang, and Y. Chai, "Blockchain and IoT based Food Traceability for Smart Agriculture," in *ICCSE'18: Proceedings of the 3rd International Conference on Crowd Science and Engineering*, 2018, no. 3, pp. 1-6, doi: 10.1145/3265689.3265692.
- [26] M. D. Borah, V. B. Naik, R. Patgiri, A. Bhargav, B. Phukan, and S. G. M. Basani, "Supply Chain Management in Agriculture Using Blockchain and IoT," *Advanced Applications of Blockchain Technology*, Singapore: Springer, 2020, vol. 60, pp. 227-242, doi: 10.1007/978-981-13-8775-3_11.
- [27] L. Augusto, R. Costa, J. Ferreira, and R. J. -Gonçalves, "An Application of Ethereum smart contracts and IoT to logistics," *2019 International Young Engineers Forum (YEF-ECE)*, 2019, pp. 1-7, doi: 10.1109/YEF-ECE.2019.8740823.
- [28] L. Hang, I. Ullah, and D. -H. Kim, "A secure fish farm platform based on blockchain for agriculture data integrity," *Computers and Electronics in Agriculture*, vol. 170, 2020, doi: 10.1016/j.compag.2020.105251.
- [29] P. W. Khan, Y. -C. Byun, and N. Park, "IoT-Blockchain Enabled Optimized Provenance System for Food Industry 4.0 Using Advanced Deep Learning," *Sensors*, vol. 20, no. 10, 2020, doi: 10.3390/s20102990.
- [30] D. J. Ghode, R. Jain, G. Soni, S. K. Singh, and V. Yadav, "Architecture to Enhance Transparency in Supply Chain Management using Blockchain Technology," *Procedia Manufacturing*, vol. 51, pp. 1614-1620, 2020, doi: 10.1016/j.promfg.2020.10.225.
- [31] S. -S. Kuo and W. -T. Su, "A Blockchain-Indexed Storage supporting Scalable Data Integrity in Supply Chain Traceability," *2020 IEEE International Conference on Smart Internet of Things (SmartIoT)*, 2020, pp. 348-349, doi: 10.1109/SmartIoT49966.2020.00064.
- [32] S. Suhail, R. Hussain, A. Khan, and C. S. Hong, "Orchestrating product provenance story: When IOTA ecosystem meets electronics supply chain space," *Computers in Industry*, vol. 123, 2020, doi: 10.1016/j.compind.2020.103334.
- [33] S. F. Aghili, H. Mala, C. Schindelhauer, M. Shojafar, and R. Tafazolli, "Closed-loop and open-loop authentication protocols for blockchain-based IoT systems," *Information Processing & Management*, vol. 58, no. 4, 2021, doi: 10.1016/j.ipm.2021.102568.
- [34] A. A. N. Patwary, A. Fu, S. K. Battula, R. K. Naha, S. Garg, and A. Mahanti, "FogAuthChain: A secure location-based authentication scheme in fog computing environments using Blockchain," *Computer Communications*, vol. 162, pp. 212-224, 2020, doi: 10.1016/j.comcom.2020.08.021.
- [35] Y. Mirsky, T. Golomb, and Y. Elovici, "Lightweight collaborative anomaly detection for the IoT using blockchain," *Journal of Parallel and Distributed Computing*, vol. 145, pp. 75-97, 2020, doi: 10.1016/j.jpdc.2020.06.008.
- [36] U. Guin, P. Cui, and A. Skjellum, "Ensuring Proof-of-Authenticity of IoT Edge Devices Using Blockchain Technology," *2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, 2018, pp. 1042-1049, doi: 10.1109/Cybermatics_2018.2018.00193.
- [37] G. Dittmann and J. Jelitto, "A Blockchain Proxy for Lightweight IoT Devices," *2019 Crypto Valley Conference on Blockchain Technology (CVCBT)*, 2019, pp. 82-85, doi: 10.1109/CVCBT.2019.00015.
- [38] M. Yavari, M. Saffkhani, S. Kumari, S. Kumar, and C. -M. Chen, "An Improved Blockchain-Based Authentication Protocol for IoT Network Management," *Security and Communication Networks*, vol. 2020, pp. 1-16, 2020, doi: 10.1155/2020/8836214.
- [39] Z. Liu and Z. Li, "A blockchain-based framework of cross-border e-commerce supply chain," *International Journal of Information Management*, vol. 52, 2020, doi: 10.1016/j.ijinfomgt.2019.102059.
- [40] S. Malik, V. Dedeoglu, S. S. Kanhere, and R. Jurdak, "TrustChain: Trust Management in Blockchain and IoT Supported Supply Chains," *2019 IEEE International Conference on Blockchain (Blockchain)*, 2019, pp. 184-193, doi: 10.1109/Blockchain.2019.00032.
- [41] P. Saindane, Y. Jethani, P. Mahtani, C. Rohra, and P. Lund, "Blockchain: A Solution for Improved Traceability with Reduced Counterfeits in Supply Chain of Drugs," *2020 International Conference on Electrotechnical Complexes and Systems (ICOECS)*, 2020, pp. 1-5, doi: 10.1109/ICOECS50468.2020.9278412.
- [42] P. Cui, J. Dixon, U. Guin, and D. Dimase, "A Blockchain-Based Framework for Supply Chain Provenance," in *IEEE Access*, vol. 7, pp. 157113-157125, 2019, doi: 10.1109/ACCESS.2019.2949951.
- [43] S. Malik, S. S. Kanhere, and R. Jurdak, "ProductChain: Scalable Blockchain Framework to Support Provenance in Supply Chains," *2018 IEEE 17th International Symposium on Network Computing and Applications (NCA)*, 2018, pp. 1-10, doi: 10.1109/NCA.2018.8548322.
- [44] M. I. S. Assaqtly *et al.*, "Private-Blockchain-Based Industrial IoT for Material and Product Tracking in Smart Manufacturing," *IEEE Network*, vol. 34, no. 5, pp. 91-97, 2020, doi: 10.1109/MNET.011.1900537.
- [45] M. R. Baharon, Q. Shi, M. F. Abdollah, S. M. W. M. S. M. M. Yassin, and A. Idris, "An Improved Fully Homomorphic Encryption Scheme for Cloud Computing," *International Journal of Communication Networks and Information Security (IJCNIS)*, vol. 10, no. 3, 2018, doi: 10.17762/ijcnis.v10i3.3573.
- [46] S. Moin, A. Karim, Z. Safdar, K. Safdar, E. Ahmed, and M. Imran, "Securing IoTs in distributed blockchain : Analysis, requirements and open issues," *Future Generation Computer Systems*, vol. 100, pp. 325-343, 2019, doi: 10.1016/j.future.2019.05.023.
- [47] S. Jangirala, A. K. Das, and A. V. Vasilakos, "Designing Secure Lightweight Blockchain-Enabled RFID-Based Authentication Protocol for Supply Chains in 5G Mobile Edge Computing Environment," in *IEEE Transactions on Industrial Informatics*, vol. 16, no. 11, pp. 7081-7093, 2020, doi: 10.1109/TII.2019.2942389.
- [48] P. Singh, M. Masud, M. S. Hossain, and A. Kaur, "Cross-domain secure data sharing using blockchain for industrial IoT," *Journal of Parallel and Distributed Computing*, vol. 156, pp. 176-184, 2021, doi: 10.1016/j.jpdc.2021.05.007.

BIOGRAPHIES OF AUTHORS






Umi Nabilah Badrol Said    She is a postgraduate student at Universiti Teknikal Malaysia Melaka, UTeM (Master), and is working as a graduate research assistant for a collaborative research grant (CRG) UTM-National 2019. She also finishes her undergraduate study for a Bachelor of Computer Science in Computer Security from Universiti Teknikal Malaysia Melaka, UTeM. She also wrote and published another paper entitled “A review on blockchain technology: a case study in fish supply chain”. Her field of interest are cryptography, elliptic curve cryptography, mobile sensing system, mobile nodes, the Internet of things, supply chains, information technology and blockchain. She can be contacted at email: uminabilah10@gmail.com.






Mohd Rizuan Baharon    He has a Ph.D. in Computer Science (Mobile Network and Cloud Security), LJMU, Liverpool, UK. M.Sc. in Mathematics (Pure Mathematics), Universiti Teknologi Malaysia, Skudai, Johor Bahru, Johor, Malaysia. B.Sc. in Industrial Mathematics, Universiti Teknologi Malaysia, Skudai, Johor Bahru, Johor, Malaysia. Currently, he is a Senior Lecturer at the Department of Computer System and Communication, Faculty of Information and Communication Technology, UTeM, Malaysia. His research interests are mainly in Mobile Network Security, Cloud Computing Security, Data Privacy, and Integrity, Mobile Users Accountability He can be contacted at email: mohd.rizuan@utem.edu.my.






Mohd Zaki Mas'ud    He has a PhD in Computer Science From Universiti Teknikal Malaysia Melaka in 2020, Masters in IT (Computer Science) From UniversitiKebangsaan Malaysia in 2005, Bachelor of Engineering (Hons) in Electronics from Multimedia University in 2000. Mohd Zaki is a Senior Lecturer in Computer and Communication System, teaching theory and practical in Honours Core Subject, IT and Network Security. 10 years in the academic world has given him skill in technical writing and has developed his passion for writing technical papers. He can be contacted at email: zaki.masud@utem.edu.my.



Ariff Idris    He has a Master in Information Technology (Computer Science) (UKM), BSc. (Hons) Information Technology (UiTM Shah Alam), Adv. Dip. in Information Technology (UniKL-IIM), NCC International Dip. in Computer Studies (NCC, United Kingdom). He is a senior lecturer in the Faculty of Information and Communication Technology, Universiti Teknikal Malaysia Melaka, Malaysia. His field of specialization are wireless technology, networking, and data communication. He can be contacted at email: miariff@utem.edu.my.



Noor Azurati Ahmad Salleh    She works as an Associate Professor in Kuala Lumpur at the Universiti Teknologi Malaysia. She graduated from Universiti Teknologi Malaysia with a B.Eng. in Computer Engineering in 2001 and a Master of Electrical Engineering in 2006. In 2013, she received her Ph.D. in Embedded Systems from the University of Leicester. Her primary areas of research interest are embedded real-time systems, cyber-physical systems (CPS), the Internet of Things (IoT), mobile and pervasive computing, as well as all aspects of software architecture, design, and testing. Smart Campus, Smart Cities, Indoor Positioning Systems, and Green ICT are the topics of her current study. She can be contacted at email: azurati@utm.my.