BLOCKCHAIN RESILIENT COMMUNICATION IN MILITARY: A SYSTEMATIC LITERATURE REVIEW

Roslinda Mohamed*[1], Hafiza Abas[2]
Farahwahida Mohd. Yusof[3]

[1, 2] Razak Faculty of Technology and Informatics, UTM, Kuala Lumpur, MALAYSIA.

[3] Pusat Penyelidikan Fiqh Sains dan Teknologi (CFiRST), UTM Johor Bahru, MALAYSIA
[1]*lindaisyahazizan@gmail.com,* [2]*hafiza.kl@utm.my*
[3]*farahwamy@utm.my*

Article history

Received:
8 December 2021

Received in revised form:
7 April 2022

Accepted:
12 May 2022

Published online:
20 May 2022

*Corresponding
lindaisyahazizan@gmail.com

Abstract

This paper provides a systematic literature review on blockchain resilient communication in the military. The aim is to investigate the current state of blockchain technology and its applications blockchain resilient communication in military perspectives. To this end, the theoretical underpinnings of numerous research papers published in high-impact academic journals over the past decade, along with several reports from the grey literature, are included in this review to facilitate our assessment and capture the ever-expanding blockchain resilient communication in military settings. Based on a structured, systematic review and thematic content analysis of the discovered literature, we present a comprehensive classification of blockchain resilient communication applications in various domains such as IoT, privacy, and data management, and introduce key themes, trends, and emerging research areas. We also highlight the shortcomings identified in the relevant literature, in particular the limitations of blockchain in robust communication technology and how these limitations play out in the military environment.

Keywords: *blockchain, military, distributed ledger technology, data management, resilient communication*

1. Introduction

A blockchain is essentially a digital ledger of transactions that is duplicated and distributed across the network of computer systems on the blockchain. The blockchain will radically change the way we live in the coming decades. Based on a peer-to-peer (P2P) topology, the blockchain is a distributed ledger technology that allows data to be stored on thousands of servers around the world and allows everyone on the network to see each other's entries in near real-time [7]. In other words, the blockchain can be described as a global online database that anyone anywhere in the world with an internet connection can use. Thus, a blockchain is owned by no one and stores information permanently on a network of personal computers. Fig 1 explain the concept of blockchain.

* *Corresponding author. lindaisyahazizan@gmail.com*

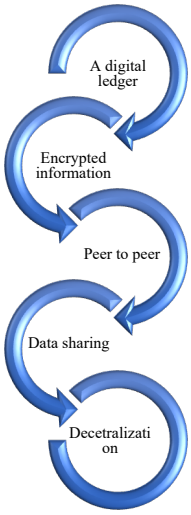

Fig 1: Concept of Blockchain [13]

Another important concept of blockchain technology is decentralization. No computer or organization can own the chain. Instead, it is a ledger that is distributed among the nodes connected to the chain. The nodes can be all kinds of electronic devices that manage copies of the blockchain and keep the network running. Each node has its copy of the blockchain and the network must algorithmically approve each newly mined block in order for the chain to be updated, trusted and verified.

Because blockchains are transparent, every action on the ledger can be easily verified and viewed. For this reason, the blockchain is considered a trust-based process with digital signatures and keys to authorize transactions and identify participants. Once a blockchain is added to a chain, it cannot be removed or modified. It can only be added to the chain, ensuring the integrity of the data. Consequently, blockchain networks not only reduce the likelihood of compromise, but also make it much harder for an attacker to do so. Put simply, all network participants have access to the distributed ledger and immutable records of transactions. With this shared ledger, transactions are recorded only once, eliminating the duplication of effort typical of traditional business networks. No participant can alter or falsify a transaction after it has been recorded in the shared general ledger.

Blockchain technology is of great use in the military environment as it can be used in both operational and support functions. Blockchain is of great use in the defense environment as it can be used in both operational and support functions: Cyber defense and data integrity, supply chain management, and resilient communications [4]. In this paper focusing SLR to resilient communication in the military as Fig 2. Technically, in the military environment, the private blockchain seems to be the most useful. With a public blockchain, access to the chain would not be controlled, which could be dangerous for the protection of sensitive information. Since private blockchains are characterized by access barriers and an administration is responsible for admitting participants and setting the rules of the chains (read and write permissions), they are best suited for military purposes. Access and system rules could be controlled by a single entity. A hybrid blockchain would also be possible in the context of inter-service governance.

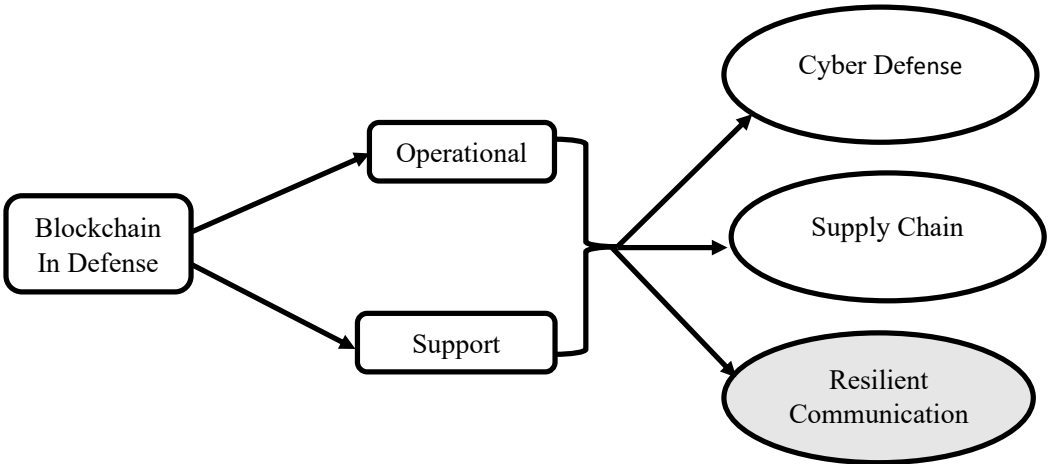

Fig 2: Block in Defense (Barnas, 2016)

This article addresses the existing literature on the use of blockchain as a supporting technology for resilient communications applications in the military, including business areas related to data privacy, security, integrity, and accountability, as well as its use in networked devices such as the Internet of Things (IoT). To achieve this goal, we will critically review existing work and studies on blockchain resilient communication in the military and use our findings to develop new directions.

1.1 Prior Research

In particular, with respect to blockchain in the context of resilient communication in the military environment, to our knowledge there seem to be very few systematic literature reviews (SLR). One of the most recent research projects in the field of blockchain data management in the military environment was conducted by [2]. In this paper, the authors show how blockchain works and discuss its military uses. They also show how numerous defense ministries around the world are working to implement blockchain technology for defense and security purposes.

Moreover, it is analyzed that blockchain, like any other new technology, still has its shortcomings. This leads us to the question of whether blockchain has the potential to be a real game-changer in military affairs, whether it has been researched thoroughly enough, and whether enough resources have been allocated to its optimization. That being said, a small number of studies have been published on blockchain and its broader implications. We will discuss them below to explore the differences between the authors' chosen topics and our research.

Storing large amounts of highly sensitive information in the same place is particularly risky. This can lead to the "terabyte of death," a term used to describe the theft of massive amounts of classified information by foreign actors. In this context, the resilience of the blockchain, with its distributed nature and ability to detect and block any attempt at the intrusion, can be very helpful. On the battlefield, soldiers need to be sure that the orders and information they receive are valid and accurate. A centralized unit that is responsible for digital communications is more vulnerable to attacks that can result in communications being intercepted or altered. Moreover, if any part of the network is affected, the integrity of the system is not

guaranteed and the entire network may collapse. Again, blockchain appears as a solution to this challenge.

All of the above studies answer questions related to the broader use of blockchain technology, but they do not specifically explore its use to improve resilient communication solutions in the military. The field of research related to blockchain has a relatively short history and is rapidly evolving. Therefore, it is necessary to provide a new summary of recent research, particularly in the area of blockchain resilient communication in the military environment, to guide new research activities.

1.2 Research Goals

The purpose of this study is to analyze the existing research and its results, and to summarize the research efforts in the field of blockchain applications for the military. To focus the work, we developed two research questions as shown in Table 1.

Table 1: Research questions

No	Research Questions (RQ)	Discussion
1	What are the latest blockchain applications focused on military resilient communications?	An overview of the latest practical applications will help you understand the impact of blockchain technology on the military.
2	How is blockchain being used to improve in military resilient communications?	Blockchain features can be used to solve problems related to devices, networks and their users the in military. This will provide an understanding of the methods used to implement blockchain in resilient communications.

1.3 Contribution and Layout

This SLR complements existing research and offers those interested in blockchain in the military domain the following contributions to advance their work:

i. We identified 58 primary studies on blockchain and resilient communication by early 2021. Other researchers can use this list of studies to advance their work in this particular area.
ii. We also select 5 primary studies that meet the quality assessment criteria we have established. These studies can provide suitable benchmarks for comparative analysis with similar research.

iii. We conduct a comprehensive review of the data contained within the subset of 5 studies and present the data to express the research, ideas and considerations in the fields of blockchain and resilient communications in military.
iv. We present a meta-analysis of state of art regarding the methods by which blockchain can be implemented to improve the resilient communications in military and emerging IoT technologies.
v. We provide representations and recommendations to support further work in this area.

This paper is structured as follows: Section 2 describes the methods which the primary studies were systematically selected for analysis. Section 3 presents the findings of all the selected primary studies. Section 4 discusses the findings related to the research questions presented earlier. Section 5 concludes the study and provides some suggestions for future research.

2. Research Methodology

To achieve the objective of answering the research questions, we conducted the SLR following the guidelines published by [5]. We attempted to iterate through the planning, implementation, and reporting phases to allow for a thorough evaluation of the SLR.

2.1 Selection of primary studies

Primary studies were highlighted by entering keywords into the search function of a specific publication or search engine. Keywords were chosen to encourage the appearance of research that would help answer the research questions. Boolean operators were limited to AND and OR. The search strings were:

("Blockchain" **OR** "Block-chain" **OR** "Distributed Ledger") **AND** ("Resilient- Communication" OR "Resilient-Communication" **OR** "Military")

The platforms searched were:

i. IEEE Xplore Digital Library
ii. ScienceDirect
iii. SpringerLink
iv. ACM Digital Library
v. Google Scholar

Searches were conducted by title, keywords, or abstract, depending on the search platform. The searches were conducted on 15 November 2021 and we processed all studies published up to this date. The results of these searches were filtered using the inclusion and exclusion criteria presented in Section 2.2. The criteria allowed us to create a set of results that could then go through the snowballing process described by [8]. Iterations of the snowball process were run

backwards and forwards until no further papers were found that met the inclusion criteria.

2.2 Inclusion and exclusion criteria

Studies to be included in this SLR must report empirical findings and could be papers on case studies, new technical blockchain applications and commentary on the development of existing security mechanisms through blockchain integration. They must be peer-reviewed and written in English. All Google Scholar results will be reviewed for compliance with these criteria, as there is a possibility that Google Scholar will provide substandard work. Only the most recent version of a study will be included in this SLR. The main inclusion and exclusion criteria are listed in Table 2.

Table 2: Inclusion and exclusion criteria for the primary studies.

No	Criteria for Inclusion	Criteria for Exclusion
1	The paper must include empirical data on the application and use of blockchain in military resilient communications	Papers addressing the economic, business, or legal implications of blockchain applications.
2	The paper must include information about blockchain or related distributed ledger technologies or resilient communications.	Grey literature such as blogs and government documents
3	The paper must be a peer-reviewed article published in conference proceedings or journal.	Non-English papers

2.3 Selection results

The initial keyword search on the selected platforms identified a total of 168 studies. This number reduced to 58 after duplicate studies were removed. After reviewing the studies against the inclusion/exclusion criteria, 58 papers remained to be read. The 58 papers were read in full, with the inclusion/exclusion criteria re-applied, and 5 papers remained. Forward and backward snowballing identified a further 1 and 2 papers respectively, so the final number of papers to be included in this SLR was 8. Figure 3 shows the number of papers selected at each stage of the process and the attrition rate of papers obtained from the initial keyword search on each platform to the final selection of primary studies.

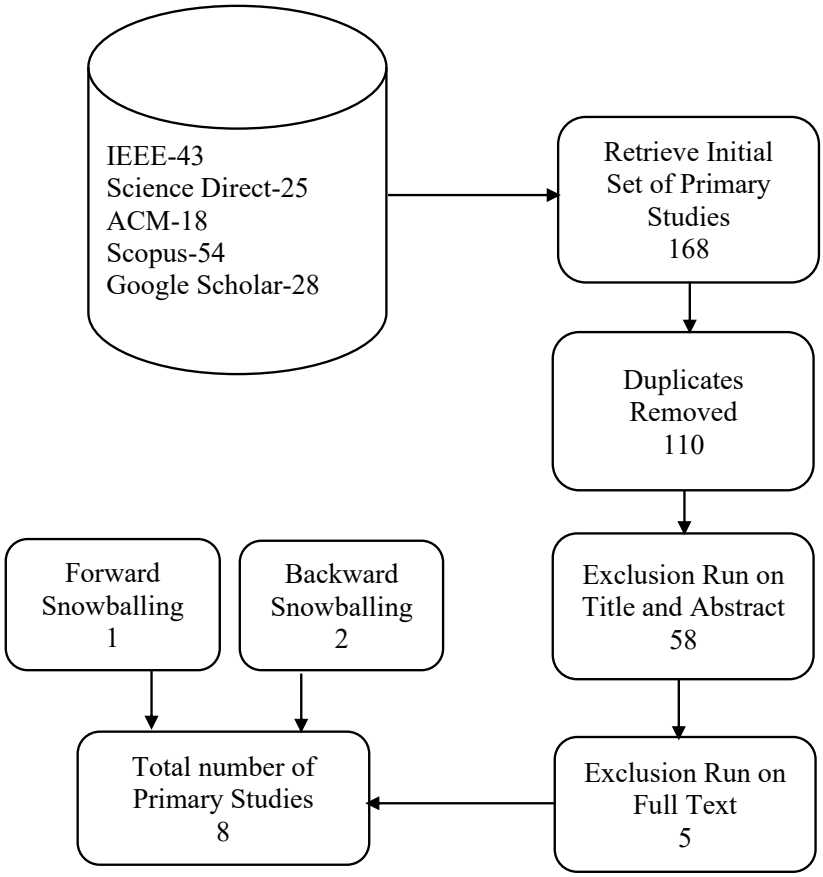

Fig 3: Attrition of papers through processing

2.4 Quality assessment

The quality of the primary studies was assessed according to the guidelines of [5]. This enabled an assessment of the relevance of the work to the research questions, taking into account any evidence of research bias and the validity of the experimental data. The evaluation process was based on the procedure used by [10]. Five randomly selected papers were subjected to the following quality assessment procedure to check their effectiveness.

2.5 Data extraction

For all papers that passed the quality assessment, data were extracted to assess the completeness of the data and to verify the accurate recording of the information contained in the papers. The data extraction process was initially tested on five studies before being extended to all studies that had passed the quality assessment. Data from each study were extracted, categorized and then stored in a spreadsheet. Data were categorized as follows:

Context data: Information about the purpose of the study.
Qualitative data: Findings and conclusions provided by the authors.
Quantitative data: When applied to the study, data observed by experimentation and research.

2.6 Data analysis

To achieve the goal of answering the research questions, we compiled data from the qualitative and quantitative data categories. In addition, we conducted a meta-analysis of those papers that went through the final data extraction process.

2.6.1 Publications over time

Although the concept of blockchain in the context of Bitcoin was published as early as 2008, there were no definitive primary studies in the military environment before 2018. In the military environment, blockchain began to emerge in 2018. Countries with major powers such as the United States, China, and Russia began to show great interest in blockchain. These countries began to discover vulnerabilities in managing their military data. Therefore, they need powerful tools to protect themselves from cyber-attacks. As mentioned earlier, blockchain can be used in the military world for operations or support tasks. This may illustrate how new the ideas are regarding applications for blockchain. Fig. 4 is a chart showing the Table 2 number of primary studies published annually. As can be seen in the figure, there is an upward trend in the use of blockchain in the military environment. We expect that there will be a significant number of research studies on the use of blockchain in real-world applications in the future, especially in the military domain as the number of publications decreases by 2021 compared to the total number of publications in 2020.

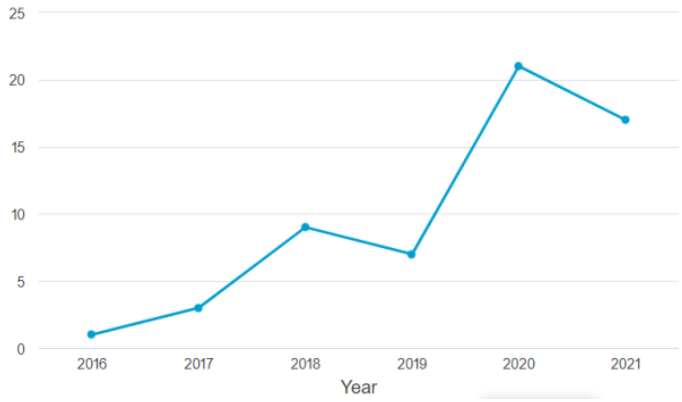

Fig. 4. Number of primary studies published over time.

2.6.2 Significant keyword counts

To summarize the common themes of the selected primary studies, an analysis of the keywords in all 10 studies was performed. Table 4 shows the frequency with which certain words occurred in all primary studies. As can be seen from the table, the third most frequently occurring keyword in our dataset, after "network" and "transaction", is the keyword "military", "IoT", excluding the keywords selected by the author, i.e., "blockchain" and "resilient communication". This shows that there is an increasing interest in the adoption of blockchain in the context of the Internet of Things (IoT), as we will discuss in more detail in Section 3.

Table 4: Keyword counts from the primary studies

No	Keyword	Count
1	Blockchain	533
2	Resilient Communication	482
3	Military	473
4	IoT	450
5	Network	450
8	Applications Requirement	430
9	Antennas	391
10	5G Mobile Communication System	333
11	Military Vehicles	320
12	Collaborative Work	222
13	Communication Cost	156

3. Findings

Each primary research paper was read in its entirety and relevant qualitative and quantitative data were extracted and summarized in Table 5. All primary studies had a focus or theme related to how blockchain deals with a particular problem. The focus of each paper is also listed in Table 5.

Table 5: Main findings and themes of the primary studies.

Primary Study	Key Qualitative & Quantitative Data Reported	Types of Resilient Communication Applications
S1	The critical communication systems such as satellites, undersea cables or tactical datalinks [4].	Secure messaging platform
S2	Position paper highlights the increasing importance of blockchain application to IoT in Army battlefields [7].	IoT
S3	Data integrity enabled by blockchain [23].	Data Storage
S4	Making them more transparent, secure and efficient [2].	Smart contract
S5	Discuss the strengths of blockchain in improving resilient communications in the military, especially with IoT [25].	IoT
S6	Proposed use of Blockchain for secure file sharing between nodes [6].	Network

S7	Blockchain-based distribution of hash search indexes to enable keyword searches in encrypted data [26].	Security Protocol
S8	Focus on IoT data trading, access, and privacy. Proposing a blockchain solution for both to provide solutions for data protection [4].	IoT

The focus of each paper was further categorized to allow for a simplified classification of the themes of the primary studies. Studies that focused on secure messaging platforms, networks, and IoT. Studies that focused on peer-to-peer sharing, encrypted data storage and search were grouped into the data storage and exchange category.

4. Discussion

4.1 What are the latest blockchain applications focused in military resilient communication?

Secure Messaging Platform. The goal of this project was to transfer messages to a decentralized protocol. In the military, resilient communications are especially useful during operations. During these operations, network access is obviously required. In the event of a highly charged conflict, blockchain could also provide robust communications. Departments of Defense should be prepared for adversary attacks on the electromagnetic spectrum during this type of conflict, especially on key communications systems such as satellites, submarine cables, and tactical data links [4]. In addition, adversaries will attempt to spoof data to disrupt the kill chain. To counter this threat, armies must be able to securely generate, protect, and share data. Blockchain networks are uniquely capable of providing these capabilities.

Application 3D Printing. Due to its distributed nature, blockchain can serve as a more secure medium for data transmission. It is increasingly being used to build structures, drones, grenade launchers, body amour, and other equipment.

4.2 How is blockchain used to improve in military resilient communication?

Personal data confidentiality. It is possible to maintain the confidentiality of personal data while making it faster and more efficient. Creating trackers for fighters could be especially useful in a defensive situation. These trackers would be distributed to all units and could be searched by all parties, allowing for instant real-time verification of the soldiers' whereabouts on the battlefield.

Blockchain technology can provide resilient communications in a highly contested environment. In a highly contentious context, blockchain technology can enable persistent communication. In a high-level battle, the military should expect adversaries to attack the electromagnetic spectrum, especially against key

communications systems such as satellites, submarine cables, and tactical data links. Adversaries will also attempt to corrupt the data used to complete the chain of death. To counter this threat, you must be able to generate, protect, and share data in a secure manner that is not compromised by adversary operations. Blockchain networks are the only ones that can provide these capabilities. Bitcoin uses a peer-to-peer messaging system that sends any message to any active node in the world within seconds. This service is supported by every node on the Bitcoin network, including smartphones. If a node's terrestrial, wireless, or satellite Internet access fails, a Bitcoin message can be transmitted via high-frequency radio, fax, or even a barcode written in one's hand.

5. Conclusion and future work

As mentioned earlier, blockchain technology has the ability to transform the way we live and conduct military operations, both operationally and logistically. Due to the decentralized and transparent nature of the blockchain concept, it has the potential to improve decision making by military officials while improving the outcomes of military operations. The advancement of blockchain technology can help shape future military logistics and planning by increasing the trust and availability of data. The defense research community is expected to look for new applications for the military based on blockchain technology in the coming years, focusing on areas such as cyber defense, secure messaging, resilient communications, logistics support, and connecting the Internet of Things. Thanks to Blockchain, military logistics will be easier and communications will be more secure. Blockchain is now being used to strengthen and improve the efficiency of the armed forces. In the long run, blockchain will be a revolution in the military if it is implemented properly and many additional military applications are discovered, as well as if it is used wisely and cost-effectively. To achieve this and gain a better understanding of the range of blockchain technologies available to address tactical challenges, the military should explore the potential of blockchain solutions for issues such as in-transit transparency, data integrity, additive manufacturing, large-scale 3D printing, reporting, operational contracting, quantum blockchain for resilient communications, and logistical estimation.

Acknowledgments

We would like to thank UTM Transdisciplinary Research Grant (**PY/2018/03456)** from Universiti Teknologi Malaysia and Malaysian Armed Forces.

References

[1] A. Lei, C. Ogah, P. Asuquo, H. Cruickshank and Z. Sun (2016). “A secure key management scheme for heterogeneous secure vehicular communication systems”. In: ZTE Communications 21.

[2] Antonios Litke, Dimosthenis Anagnostopoulos. Blockchains for Supply Chain Management (2018): Architectural Elements and Challenges Towards a Global Scale Deployment.

[3] Babich, V., G. Hilary (2018). What OM researchers should know about blockchain technology. Working Paper

[4] Barnas, Blockchains in National Defense: Trustworthy Systems in A Trustless World, 2016.

[5] B Kitchenham(2004). Procedures for performing systematic reviews Keele, UK, Keele University

[6] Bayu Adhi Tama, Bruno Joachim Kweka (2017). A Critical Review of Blockchain and Its Current Applications International Conference Electrical Engineering and Computer Science.

[7] Cisco. “The Internet of Things [INFOGRAPHIC].” blogs@Cisco - Cisco Blogs. Accessed March 17, 2016. http://blogs.cisco.com/diversity/the-internet-of-things-infographic.

[8] C. Wohlin, Guidelines for snowballing in systematic literature studies and a

replication in software engineering, in: Proc. 18th Int. Conf. Eval. Assess. Softw.Eng. - EASE 14, 2014, p. 110.
[9] Driscoll, Kevin, Brendan Hall, Håkan Sivencrona, and Phil Zumsteg (2003). "Byzantine Fault Tolerance, from Theory to Reality." In Computer Safety, Reliability, and Security, edited by Stuart Anderson, Massimo Felici, and Bev Littlewood, 235–48. Lecture Notes in Computer Science 2788. Springer Berlin Heidelberg.
[10] Douceur, John R. "The Sybil Attack - Microsoft Research." Proceedings of 1st International Workshop on Peer-to-Peer Systems. Accessed April 4, 2016., http://research.microsoft.com/apps/pubs/default.aspx?id=74220.
[11] Hubert Pun, Jayashankar M. Swaminathan (2018). Blockchain Adoption for Combating Deceptive Counterfeits. https://ssrn.com/abstract=3223656
[12] I. Omame, Juliet C. Alex-Nmecha, Application of Blockchain in Libraries and Information Centers Published 2021, Computer Science,Advances in Library Information Science.
[13] Iyolita Islam, Kazi Md. Munim (2020). A Critical Review of Concepts, Benefits, and Pitfalls of Blockchain Technology Using Concept Map. https://ieeexplore.ieee.org
[14] Kaushal, Mohit, and Sheel Tyle (2016). "The Blockchain: What It Is and Why It Matters." The Brookings Institution. Accessed. http://www.brookings.edu/blogs/techtank/posts/2015/01/13-blockchain-innovation-kaushal.
[15] Kevin A. Clauson, Elizabeth A. Breeden (2020) Leveraging Blockchain Technology to Enhance Supply Chain Management in Healthcare: An Exploration of Challenges and Opportunities in the Health Supply Chain. https://doi.org/10.30953/bhty.v1.20
[16] Mohamed Ali Kandi1, Djamel Eddine Kouicem(2020), A Blockchain-based Key Management Protocol for Secure Device-to-Device Communication in the Internet of Things. IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications.
[17] Paul J. Taylor (2020). A systematic literature review of blockchain cyber security.https://doi.org/10.1016/j.dcan.2019.01.005.
[18] SigmaLedger (2018). Challenges of Blockchain adoption for anti- counterfeit solution. SigmaLedger, accessed at https://blog.sigmaledger.com/challenges-of-blockchain-adoption-for-anti- counterfeit-solution-8b53e1e18c23
[19] Shireesh Aptea, Nikolai Petrovskyb (2016), Will blockchain technology revolutionize excipient supply chain management? IPEC-Americas Journal Manoshi Das Turjo (2020). Smart Supply Chain Management Using the Blockchain and Smart Contract. https://doi.org/10.1155/2021/6092792
[20] Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. Decentralized Business Review, 21260.
[21] S. Hosseini, B. Turhan, D. Gunarathna, A systematic literature review and meta-analysis on cross project defect prediction, IEEE Trans. Softw. Eng. 45 (2) (1 Feb 2019) 111–147.
[22] "The DoD Cyber Strategy." Department of Defense, April 1, 2015.
[23] U.S. Joint Chiefs of Staff. "Joint Publication 3-12 (R), Cyberspace Operations. Accessed April 6, 2016. http://www.dtic.mil/doctrine/new_pubs/jps_12R.
[24] W. Creswell & Plano Clark (2018) Designing and conducting mixed methods research. 3rd ed. Washington, D.C.: Sage Publications; 2017
[25] Work, Robert O. "Reagan Defense Forum: The Third Offset Strategy." U.S. Department Of Defense. Accessed March 17, 2016. http://www.defense.gov/News/Speeches/Speech
[26] Yanni Yang (2019). Data Management in Supply Chain Using Blockchain: Challenges and a Case Study. https://www.researchgate.net/publication
[27] Y. Gupta, R. Shorey, D. Kulkarni, J. Tew, The applicability of blockchain in the Internet of Things, in: 2018 10th Int. Conf. Commun. Syst. Networks, 2018,p. 561564.
[28] Zetter, Kim (2018). "NSA Hacker Chief Explains How to Keep Him Out of Your System." WIRED. http://www.wired.com/2016/01/nsa-hacker-chief-explains-how-to-keep-him-out-of-your-system/.