TEST Engineering & Management

May – June 2020
ISSN: 0193-4120 Page No. 1131 - 1138

Literature Review of Blockchain-Based Technology for Data Storage Systems in the Governmental Organization

[1]Fikroh Amali Fahmi Addiani,
[1] Department of Civil Engineering, Faculty of Engineering, Universitas Indonesia, Salemba, Indonesia
[1]fahmiaddi@yahoo.co.id

Article Info
Volume 83
Page Number: 1131 - 1138
Publication Issue:
May - June 2020

Article History
Article Received*: 11August 2019*
Revised*: 18November 2019*
Accepted*: 23January 2020*
Publication*: 10 May2020*

Abstract:

Cloud computing-based as a data storage system is one of the most widely used systems in government organizations. However, the most problem in this system is the issue of data security. Based on the literature studies, blockchain technology can be used as a data storage system with a higher level of security compared to the cloud computing system. This paper reviews twenty-four studies around the world which had identified the weakness of cloud storage systems, also the characteristics and advantages of blockchain technology. The purposes of this paper are to identify and communicate the research gap in the previous literature. To achieve that purpose, the author has conducted a comprehensive literature review. The twenty-four articles were reviewed in five discussion topics: data storage system base on cloud computing, security in data storage systems, blockchain and the characteristics, blockchain as a base data storage system, and utilization of blockchain technology.

Keywords: *data security, cloud storage, governmental organizational, blockchain technology*

I. INTRODUCTION

Cybersecurity or information technology security involves protecting and minimizing disruption of aspects of confidentiality, integrity, and availability [1] of information assets including the use, storage or transmission of information through the application of policies, education, and technology [2].

Cybersecurity threats also occur in government organizations. According to data from the IBM X-Force Threat Intelligence Index 2019, Government Organizations are ranked seventh for the industry with the greatest cybersecurity threat (8%). Violations that occur include the use, sale, and transmission of information, primarily for economic and political gain.

Government organizations manage a lot of confidential critical data and information. To safeguard data and information from all threats, a data and information storage system are needed that is qualified in terms of security, access, and provision of information quickly and accurately.

Security in sharing data is vulnerable to cyber-attacks. Existing data is increasing every year, so it is important to pay attention to aspects of infrastructure, confidentiality storage, and security of data stored and the integration of old data in larger storage media [5].

In traditional database systems such as cloud storage, data control is centralized so that it does not guarantee the confidentiality, integrity, and authenticity of the data. This requires distributed data storage technology that can guarantee the authenticity, confidentiality, and integrity of data [6].

Based on the 2018 Cloud Readiness Index (CRI), the results of the 2018 Asia Cloud Computing Association research, Indonesia ranks 11th with a total value of 49.4 out of 100 when compared to countries in the Asia Pacific region for the growth of cloud computing-based storage media [3].

Indonesia should prioritize initiatives to improve cloud computing infrastructure such as by increasing broadband speeds and providing more reliable electricity.

Also, despite experiencing the addition of data center infrastructure every year but it is not

May – June 2020
ISSN: 0193-4120 Page No. 1131 - 1138

significant enough to meet the needs of cloud computing in Indonesia, especially for government organizations. Confidential documents owned by the Government of Indonesia require data centers that must be managed by the Government themselves and require a long time and high costs in its development [4].

Cloud computing-based data storage systems have several risks including low levels of system security; data loss due to entity damage; lost data due to deletion by unauthorized persons; lost access due to entity closure/damage; lost access because there is no internet connection; lost access due to OS configuration problems; and changes or modifications to the data due to the absence of non-transparent transaction and transaction logs.

Blockchain technology is a technology that can be used for distributed data storage because it is peer-to-peer so that in the process data can be moved from one user to another without involving third parties, and all transactions are transparent and data storage is guaranteed to be secure because it is replicated throughout blockchain network [1].

This article presents information about the deficiencies in the cloud storage system that can be overcome with the advantages of the blockchain as a base data storage system.

II. RESEARCH OBJECTIVE

This paper presents a general overview of the weakness in cloud storage systems, also the characteristics and advantages of blockchain technology from related articles. The objective of this research is to identify and communicate the research gaps in the literature. The articles will be discussed in five discussion topics: data storage system based on cloud computing, security in data storage systems, blockchain and the characteristics, blockchain as a base data storage system, and utilization of blockchain technology.

III. METHODOLOGY

In this paper, the researcher used a method of analyzing academic articles through the meta-analysis classification system. That system had been partially adapted in previous research. The articles that are reviewed can be in the form of journal articles and conference papers that are related to the weakness in cloud storage systems, also the characteristics and advantages of blockchain technology. The researcher used 24 articles as objects to be reviewed. Data are collected from the articles will be divided into six discussion topics.

IV. RESULT AND FINDINGS

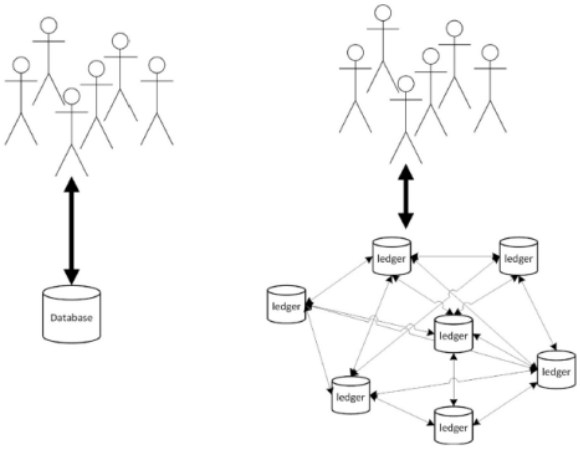
A. Cloud Computing Based Data Storage System

According to [7] based on its database (database) the data storage system can be classified into centralized, and decentralized. A centralized database is a system that organizes all data in a single node. This system is easy to manage but has low reliability and availability [8]. An example of a centralized database is cloud storage.

Whereas in a decentralized database several computers that are scattered in several locations are connected and each computer can do similar processing independently and can interact with each other in data exchange. An example of a decentralized database is blockchain [8].

Cloud storage is a data storage service system that is integrated and synchronized via the internet and can be accessed using various platforms (OSX, iOS, Windows, Windows Mobile, Android, Linux, etc.) [9].

Cloud storage is a technology developed from cloud computing, which is a computing model with resources such as processor/computing power, network storage, and software being abstracted as services on the internet network with remote access patterns [10].



May – June 2020
ISSN: 0193-4120 Page No. 1131 - 1138

Figure 2 1 Centralized Database (left) and Decentralized Database (right)
Source: Olnes, Ubacht, dan Janssen, (2017)

There are many advantages possessed by Cloud storage when compared to traditional data storage including ease of access anytime and anywhere with an internet network [11] and file sharing [9] no need to buy storage devices but only enough to pay for as much storage as used [12], allows users to access various other applications directly [13].

However, cloud storage also has several shortcomings, including the possibility of hacking, data security is not guaranteed entirely by service providers, expensive for everyday use [13].

The threat of data security in cloud computing is also conveyed by [14] in his research. Cloud computing systems should be able to provide certainty of integrity, confidentiality, privacy and data availability.

[12] summarizes some of the shortcomings of cloud storage, namely:

1. Immaturity. Vendors have to re-find solutions to resolving incompatibilities with data storage online, and that has created difficulties for the organization.
2. Price and Reliability. Users must calculate the effectiveness of the cost of hosting and maintaining data by the cloud.
3. Security. There is a possibility that data can be stolen or viewed by unauthorized persons.
4. Bandwidth limitation. If the bandwidth is not as fast as the user needs, the solution won't match.
5. Network distance (Latency). The amount of temporal delay in propagation and transmission packets in the network will affect cloud storage systems.

Besides, according to [13] caution is needed in moving documents to cloud storage because it will move permanently from the original folder to the location of cloud storage. Do a copy-paste if you want the document to remain in the original folder and cloud storage. Cloud storage also has a specific bandwidth limit, if it exceeds the limit there will be a significant increase in costs; can't access data without an internet connection.

In cloud storage, if you want to manipulate files locally through several devices, you need to download the service on all devices. The main problem with cloud storage is the problem with the security and privacy of data that is stored remotely [15].

B. Security in Data Storage System

[12] revealed that cloud storage is a service that has many shortcomings, but this is not a consideration for users for economic reasons and flexibility. Furthermore, users will lose control from the security side, and there are concerns that data is accessed by unauthorized persons.

Overall, data security covers three aspects namely confidentiality, integrity, and availability [13]:

• Confidentiality: protection of data and information from disclosure to unauthorized persons.

• Integrity: protection of data and information from being modified by unauthorized persons.

• Availability: data access whenever needed by an authorized person.

Security in a data storage system is one aspect of an Information Security Management System (ISMS). Information security includes the security of documents, hardware, software, infrastructure and buildings that protect it [16]. In the ISMS, the term information refers to information in the form of documents and data.

[16] mentions several aspects of information security including:

1. Privacy. Information collected, used and stored by the organization is used only for certain purposes, specifically for the data owner. Privacy guarantees the security of data for the owner of information from others.
2. Identification. The first step that must be met to obtain access rights to information that is secured, for example by using a username.
3. Authentication. The system can prove that a user is indeed a person who has the claimed identity.
4. Authorization. Guarantee that users have received specific and clear authorization to access, change or delete content and information.
5. Accountability. The system can present data on all activities to the information that has been done, and who is doing the activity.

Meanwhile, according to ISO/IEC 27002, 2005

May – June 2020
ISSN: 0193-4120 Page No. 1131 - 1138

documents related to ISO 27001 documents, there are seven aspects of information, namely confidentiality, integrity, availability, authenticity, accountability, non-repudiation, and reliability. Whereas information security aspects include confidentiality, integrity, and availability (CIA).

1. Confidentiality. Certain information guarantees can only be accessed by people who have the right to access them.
2. Integrity. Guaranteed completeness of information and guard against corruption, damage and other threats that cause the information to change from the original information.
3. Availability. Guaranteed information can be accessed by users at any time, without interference and not in a format that cannot be used.

Security in systems and applications is also one of the four foundations for developing a national strategy for developing cyber-security in Indonesia [17].

C. Blockchain and the Characteristics of Blockchain

Blockchain, a peer-to-peer network technology [1] originally introduced by Satoshi Nakamoto in 2008 as part of bitcoin - a virtual currency system.

As an innovation, blockchain exists to store various data and information, including financial transactions [18]. Blockchain is a database in the form of records or ledgers of all digital transactions spread across all system users [19].

Blockchain is a decentralized application, without centralized authority, without controlling entities [20], and eternal [21]. Blockchain consists of a group of nodes, where each node has the same data replication [21].

Blockchain has several characteristics, namely:

1. Decentralization. As a scattered database, each part of the blockchain has access to the entire database with complete history, and each part can verify transaction records directly without contact [22], and without authentication by a central agent [23] to avoid one party taking full control against the network [24]. In this way, blockchain can significantly reduce server costs (including development costs and operating costs) and reduce performance bottlenecks on a central server [23].
2. Peer-to-peer transmission. With blockchain, data can be moved without a third party. Communication takes place directly without going through the central node. Each node stores and forwards information to all other nodes [25].
3. Transparency through encryption. Each transaction can be seen by all users, and the blockchain will authenticate user data in real-time before the transaction is ratified (Bank Indonesia Working Paper, 2017 in Adinigsih 2019). Each node in the blockchain is unique to more than 30 identified alphanumeric characters. Users can choose to remain anonymous or provide proof of identity to others [22].
4. Data recording permanently. Transactions in a blockchain are always updated and their history cannot be changed or deleted because it is linked to every transaction record [25]. Each entity can review the information stored, but changes to the database can only be implemented by reaching consensus [26].
5. Secure. Blockchain is technology without the influence or involvement of middle people. Also, a consensus mechanism is needed to validate transactions, and authentic transactions are placed in blocks containing timestamps and hashes from the previous block [24]. So forgery can be detected easily [23]. Also, some sources say because the data is spread on various parties, blockchain is a technology that is safe in the event of a cyberattack, compared to old technology that only uses one party in storing data and information [18].
6. Digital programming based. Blockchain transactions are bound by computational and programmed logic [22].
7. Traceability. The ability to trace and track previous transactions iteratively [24].
8. Anonymity. Each user can interact with the blockchain network, to avoid exposing the user's identity it can generate many addresses. User personal information is not stored by the

May – June 2020
ISSN: 0193-4120 Page No. 1131 - 1138

central party [23].

9. Permanent. Data in the blockchain cannot be changed or deleted. Permanence works in total based on consensus [24].

D. Blockchain Types

[24] divides blockchain into three types, namely public blockchain, private blockchain, and consortium blockchain.

1. A public blockchain is a blockchain that allows all nodes to access data. For example Bitcoin and lite coins. All cryptocurrencies run a common blockchain [27].
2. Private Blockchain. Pre-registration, invitation or validation by the central authority is required, meaning only those who have permission. Generally used in intra-company or inter-business solutions [27].
3. Blockchain Consortium. Blockchain is not controlled by a single authority, but rather by a group of approved authorities. Blockchain consortium is semi-decentralized.

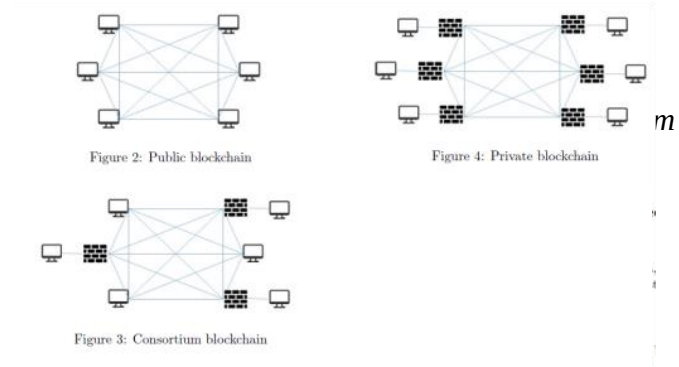


Figure IV-1 Blockchain Types
Source: (Lin & Chun Liao, 2017)

F. Blockchain as the Base of Data Storage System

[23] emphasized that Blockchain can function as data management as well as data analysis. As data management, blockchain can be used to store important data because it is distributed and secure. Besides, blockchain can also ensure data authenticity. For example for patient information data, it cannot be tampered with and is difficult to steal.

In terms of data analysis, transactions on the blockchain can be used for analysis. For example, by extracting trading pattern data, users can predict the behavior of their potential partners with analysis.

Based on the results of his research [28] showing the potential benefits of blockchain which are summarized from various literature and displayed in the following table:

Benefit	Explanation
Strategy	
Transparency	Transaction history remains visible and each node has a complete picture of transactions.
Avoiding fraud and manipulation	Illegal changes are difficult because the information is stored in lots of distributed ledger.
Reducing corruption	Storage in the blockchain prevents corruption because data is difficult to manipulate.
Organization	
Increase trust	Verification of data with multiple nodes and unchanging recording improves data control.
Transparent and auditable	Able to track transaction history and make audit trails.
Improve predictive capability	Information history availability improve predictive ability.
Increase control	Need for agreement to add transactions increases control.
Clarity of ownership	Governance needs to be clearly defined and how information can be changed.
Economy	
Reducing costs	The cost of validating transactions can be reduced because it does not involve humans.
Increased resistance to spam and DDOS attacks	Higher levels of resilience and security reduce the cost of attack prevention.
Information	
Data integrity and improvement in data quality	Information stored according to what is represented in reality is due to the need for consensus and its distributed nature. This results in higher data quality.
Reducing human errors	Transactions and controls automatically reduce human errors
Access to information	Information is stored in many

May – June 2020
ISSN: 0193-4120 Page No. 1131 - 1138

Benefit	Explanation
	places which can increase convenience access and access speed.
Privacy	User privacy can be anonymous by providing an encryption key or access, to prevent others from seeing the information.
Reliability	Data is stored in many places. The consensus mechanism ensures that information can only be changed when all parties concerned agree.
Technology	
Resilience	Resilient against crime
Security	Because data is stored in many databases using encryption, it is more difficult to manipulate. The possibility of hacking at the same time is very small.
Persistence and irreversibility	After data are written to the blockchain, it is difficult to change or delete it.
Reducing energy consumption	Network energy consumption is reduced by increasing efficiency and transaction mechanisms.

Source: Svein Ølnes, Jolien Ubacht, dan Marijn Janssen, (2017)

The potential benefits of the blockchain can be a solution to the problem of data storage systems, including the low level of system security, the risk of data loss due to damage, the risk of loss of access due to closure/damage to the entity, the risk of data changes due to the absence of activity logs and non-transparent transactions.

The use of blockchain will increase decentralization, data integrity, and transparency - along with increased efficiency and reduced operational costs.

Blockchain maximizes the efficiency of institutional performance Blockchain systems and smart contracts can be used to automate tasks and workflows, which can significantly reduce the time and money spent in the bureaucratic process.

In addition to reducing expenses which is very practical, this will also help to strengthen the trust and satisfaction of the community. More efficiency and reduced costs are likely to increase levels of government revenue highly. By cutting operational costs, the government can invest in other areas such as education, safety, and public health.

Blockchain is a revolution in the management process that can be a solution related to interoperability, trust, and transparency in a network or system. Under its function, blockchain is a distributed ledger of assets and transaction storage [29].

Based on the results of research Sibarani, Pramukantoro, and Bakhtiar, 2019 blockchain can know if there is data manipulation and can restore the initial state of the data as before and can maintain the integrity of the data that has been stored.

Documents in the blockchain database are less likely to be hacked or falsified because the system runs without a third party and there is algorithmic automation. Besides, with the database being split into hundreds of millions of servers, ensuring agreement automation, data is recorded in a transparent system so that the truth can be checked.

Blockchain can increase network efficiency results and increase network security [25].

G. The Utilization of Blockchain Technology in Government Organizations

Blockchain technology has attracted many stakeholders and has been applied in various sectors such as financial services and shipping [27], health, utilities, housing, government [20], banking, and public services [25], IoT, and education [24].

[29] in his research results revealed that blockchain technology can be used in government voting systems as practiced by the Danish Government. With the anonymity of voters, the record of the results of the vote will not change.

Also, it is still under research [29], conveyed that the blockchain is also applied by the government for food safety by using an application that connects farmers with markets to ensure food safety and quality.

The results of his research, [24] emphasized that the blockchain with its decentralized characteristics, transparency, and smart contracts can improve governance problems such as data privacy, food security, and elections.

Blockchain technology has been applied to many government organizations. For example in Estonia, blockchain is used in the Government Database System, medical records, civil/population registration (birth certificates and population

May – June 2020
ISSN: 0193-4120 Page No. 1131 - 1138

education data). The Dubai government began in 2020 claiming all government systems will be based on blockchain. The United States uses the blockchain for the financial system. Other uses in the agrarian sector are land registration, banking, insurance, IT, food, and logistics.

The use of blockchain technology in Indonesia based on the literature includes blockchain research as a basis for e-voting, with the advantages of blockchain which are anonymity, autonomy, confidentiality, transparency, distribution, and auditing are expected to be able to make elections go better according to the principle of direct, general, free, confidential, honest and fair [30].

[31] in his research on Blockchain as an e-commerce base in Indonesia emphasized that blockchain has the potential to resolve the challenges of fraud, commission fees, limited contacts and misuse of personal data in e-commerce by increasing security and transparency through the application of cryptocurrency in payments and smart contracts. As a result, he proposed blockchain technology as an architecture and e-commerce platform system in Indonesia.

V. CONCLUSION

This paper discusses twenty-four articles related to the weaknesses of cloud storage systems and the advantages of blockchain technology for data storage and data security. The twenty-four articles consisted of research conducted from 2013 to 2019. The following results are obtained from the literature review regarding the six discussion topics.

1. For the Cloud Computing-based Data Storage Systems, the main problem faced is a problem with data security and privacy.
2. For the security in a Data Storage System, the most important thing is confidentiality, integrity, and availability.
3. The most dominant characteristic of blockchain in a data storage system is decentralization, it can record data permanently, safely, and permanently.
4. As a Base Data Storage System, blockchain will increase decentralization, data integrity, and transparency.
5. Blockchain technology in government organizations is used for the Government Database System, medical records, civil/population registration (birth certificates and population education data), financial systems. Land registration systems, banking, insurance, IT, food, and logistics, and e-voting.

VI. LIMITATION

This paper only discusses the literature review of articles regarding the weaknesses of the cloud storage systems and the advantages of blockchain technology as the solution. The result of this paper shows the state of the art of review articles. This paper does not produce any results regarding the objectives or objectives of each review article.

REFERENCES

[1] Perdani, M. K., & Santosa, P. I. (2018). Blockchain untuk Keamanan Transaksi Elektronik Perusahaan Financial Technology (Studi Kasus pada PT XYZ). Seminar Nasional Teknologi Informasi dan Multimedia 2018 (hal. 1.14.7-12). Yogyakarta: Universitas Amikom Yogyakarta.

[2] Whitman, M. E., & Mattord, H. J. (2017). Principles of Information Security Sixth Edition. Boston: Cangage Learning.

[3] Asia Cloud Computing Association. (2018). Cloud Readiness Index 2018. ACCA.

[4] Prabu, H. K. (2019). Analisis Manajemen Proyek untuk Implementasi Penyimpanan Arsip Rahasia Negara Menggunakan Blockchain.

[5] Nugroho, F. P., Abdullah, R. W., Wulandari, S., & Hanafi. (2019). Keamanan Big Data di Era Digital di Indonesia. Informa Politeknik Indonusa Surakarta, Vol 5 No.1:28-34.

[6] A, Rajalakshmi,et al, (2018) A Blockchain and IPFS Based Framework for Secure Research. International Journal of Pure and Applied Mathematics, Volume 119 No. 15 2018, 1437-1442.

[7] Singh, I., & Won Lee, S. (2018). Comparative Requirement Analysis for the Feasibility of Blockchain for Secure Cloud. CCIS, 57-72.

[8] Lacob, N. M., & Moise, L. M. (2015). Centralized vs. Distributed Databases. Case Study. Journal of Economic Studies, 119–130.

[9] Santiko, I., Rosido, R., & Wibawa, S. A. (2017). Pemanfaatan Private Cloud Storage Sebagai

May – June 2020
ISSN: 0193-4120 Page No. 1131 - 1138

Media Penyimpanan Data E-Learning pada Lembaga Pendidikan. Jurnal Teknik Informatika Vol. 10 No. 2, 137-146.

[10] Ibrahim, M., & Kusnawi. (2013). Analisis dan Implementasi Owncloud Sebagai Media Penyimpanan pada Yayasan Salman Al-Farisi Yogyakarta. DASI, 32-37.

[11] Afdhal. (2013). Studi Perbandingan Layanan Cloud Computing. Jurnal Rekayasa Elektrika, 193-201.

[12] Obrutsky, S. (2016). Cloud Storage: Advantages, Disadvantages and Enterprise Solutions for Business. ResearchGate.

[13] Vyas, J., & Modi, P. (2017). Providing Confidentiality and Integrity on Data Stored in Cloud Storage by Hash and Meta-data Approach. International Journal of Advance Research in Engineering, Science & Technology, 38-50.

[14] Vurukonda, N., & Rao, B. (2016). A Study on Data Storage Security Issues in Cloud Computing. 2nd International Conference on Intelligent Computing, Communication & Convergence, 128 – 135.

[15] Selvananthan, N., & Poravi, G. (2018). Comparative Study on Decentralized Cloud Collaboration (DCC). International Conference for Convergence in Technology.

[16] Sarno, R., & Iffano, I. (2009). Sistem Manajemen Keamanan Informasi. Surabaya: ITSPress.

[17] Ardiyanti, H. (2014). Cyber - Security dan Tantangan Pengembangan di Indonesia. Politica, 96-110.

[18] Adiningsih, S. (2019). Transformasi Ekonomi Berbasis Digital di Indonesia. Jakarta: PT. Gramedia Pustaka Utama.

[19] Albrecht, S., Reichert, S., & Neumann, D. (2018). Dynamics of Blockchain Implementation – A Case Study from the Energy Sector. the 51st Hawaii International Conference on System Sciences, (hal. 3527-3536). Hawaii.

[20] Shetty, S. S., Kamhoua, C. A., & Njilla, L. L. (2019). *Blockchain for Distributed Systems Security*. New Jersey: IEEE Press.

[21] Sibarani, I., Pramukantoro, E. S., & Bakhtiar, F. A. (2019). Implementasi Blockchain berbasis Bigchain DB dan Tendermint pada Sistem Penyimpanan Data IoT. *Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer*, 7603-7611.

[22] Iansiti, M., & Lakhani, K. R. (2017, Januari - February). The Thruth About Blockchain. Harvard Business Report.

[23] Zheng, Z., & Xie, S. (2018). Blockchain challenges and opportunities: a survey. International Journal of Web and Grid Services, 352-375.

[24] Razzaq, A., Khan, M., Talib, R., Butt, A. D., Hanif, N., Afzal, S., & Raouf, M. R. (2019). Use of Blockchain in Governance: A Systematic Literature Review. International Journal of Advanced Computer Science and Application, Vol. 10 No. 5. 685 - 691.

[25] M. Hussein, D. E.-D., Taha, M. H., & Khalifa, N. E. (2018). A Blockchain Technology Evolution between Business Process Management (BPM) and Internet-of-Things (IoT). (IJACSA) International Journal of Advanced Computer Science and Applications, Vol.9, No.8, 442-450.

[26] Albrecht, S., Reichert, S., & Neumann, D. (2018). Dynamics of Blockchain Implementation – A Case Study from the Energy Sector. the 51st Hawaii International Conference on System Sciences, (hal. 3527-3536). Hawaii.

[27] Diordiiev, V. (2018). Blockchain Technology and Its Impact on Financial and Shipping Services. Economic Ecology Socium.

[28] Olnes, S., Ubacht, J., & Janssen, M. (2017). Blockchain in Government: Benefits and Implications of Distributed Ledger. *Government Information Quarterly 34*, 355-364

[29] Alketbi, A., Nasir, Q., & Talib, M. A. (2017). Blockchain for Government Services – Use Cases, Security Benefits and Challenges. IEEEE, 112-119.

[30] Winarno, A., Harsari, J., & Ardianto, B. (2018). Block-Chain Based E-Voting For Indonesia. *Journal of Engineering and Science Research*, 2 (5): 13-17.

[31] Ismanto, Leonando;et al. (2018). Blockchain as E-Commerce Platform in Indonesia. *Journal of Physics: Conference Series*.