

# Blockchain Technology and Implementation : A Systematic Literature Review

Henry Rossi Andrian<sup>1</sup>, Novianto Budi Kurniawan<sup>2</sup>, Suhardi<sup>3</sup>

<sup>1,2,3</sup>School of Electrical Engineering and Informatics, Institut Teknologi Bandung (ITB)  
bandung, Indonesia

<sup>1</sup>rossi@tass.telkomuniversity.ac.id, <sup>2</sup>noviantobudik@s.itb.ac.id, <sup>3</sup>suhardi@stei.itb.ac.id

**Abstract**— As research on blockchain continues to grow, blockchain technology was adopted to develop several information systems. There are many opportunities to examine the utilization of blockchain technology to be used in developing systems as needed. This paper summarizes the conditions of blockchain research in terms of technology and its implementation. This paper was written using a systematic literature review (SLR) as one of the methodologies used to solve problems by tracing the results of previous studies. The problem that you want to study in SLR is usually referred to as a research question (RQ). The defined RQ is related to the topic and clarifies each question by tracing previous research papers indexed in reputable journal databases such as IEEE Xplore, Springerlink, Scopus, and ScienceDirect. After synthesizing 41 articles, the result is: blockchain can be used in many applications, some applications that adopt blockchain technology are banking applications, e-voting applications and digital forensic applications. Often, applications that use blockchain technology only focus on developing one of the blockchain technologies that suits their needs. Some developers maximize the components of the contract on the blockchain, some further develop the data structure of the blockchain itself. The use of blockchain technology is still wide open for the implementation of other information systems. The expected contribution of this paper is to provide a general overview for researchers who want to build applications that use blockchain as a basis for researching so they can conduct further studies to better understand whether the applications they will develop are suitable for using blockchain technology as a basis.

**Keywords**—Blockchain, SLR, technology

## I. INTRODUCTION

Blockchain technology became known after bitcoin was widely used. Initially, blockchain was only used for financial and trading transactions, but several studies have shown that blockchain technology can be used to develop systems outside financial and trade transactions. This is because there is a high level of transparency in blockchain technology. For example, in Bitcoin, because wallets are in a distributed structure, the total number of coins and the volume of transactions in the world can be followed quickly and clearly. This system does not require central authority to approve or complete operations because it is P2P based.

With the development of blockchain concepts and technology, more and more people are also developing the blockchain concept, including the IEEE. IEEE has issued several standards related to blockchain technology and implementation. Some of the standards being developed by IEEE include P2418.1 - Standard for the Framework of Blockchain Use in Internet of Things (IoT) and P2418.2 - Standard Data Format for Blockchain Systems.

As time goes by, blockchain usage in fields other than cryptocurrency is growing. A research that uses blockchain in a field other than cryptocurrency is a secure e-voting system. This e-voting application uses smart contracts owned by Ethereum to protect only those who have the right to access and vote on the system. In addition to safe e-voting, the blockchain concept and technology are also implemented in digital forensic.

Blockchain is very useful and starts to be adopted in some of the current systems which include banking systems, e-voting, and IoT. To understand the concept and implementation of blockchain even further, in this paper a literature review is conducted using Systematic Literature Review (SLR). The SLR was previously used in medicine and pharmaceuticals and began to be developed for software engineering by Kitchenham and Charters [14] in 2007. SLR became the standard methodology used to find solutions by tracing the results of previous research. Problems raised in the SLR are called research questions (RQ). Some of common reasons for conducting SLRs are: summarizing existing research results, to identify gaps in current research, or to provide a framework for specific research areas. In this paper, we summarize blockchain development conditions, especially to find out the characteristics, supporting technology, and applications that are built. To get comprehensive results, we explored a number of literatures published in popular journal databases namely IEEEExplore, SpringerLink, Scopus, and ScienceDirect from 2008 to 2018.

## II. RESEARCH METHODOLOGY

The systematic literature review as a process of identifying, evaluating, and interpreting research results to provide answers to research questions [14] consists of several stages, namely: defining research questions, determining learning topics, extracting the required data, synthesizing data, and explaining the results.

Research questions are set to keep the review target. The research questions set out in this study are shown in table 1 below..

TABLE I. RESEARCH QUESTION

ID	Research Question	Motivation
RQ1	What are the blockchain technology adopted by current applications?	Identify the blockchain technology and how to develop application using blockchain.
RQ2	What are applications implemented using blockchain?	Identify the variety of application using blockchain?

To get the literature that corresponds to the research questions, from September 4<sup>th</sup>, 2018 to September 16<sup>th</sup>, 2018, tracking the results of research published in the popular journal database using a specific search string is carried out. The search strings used in finding the appropriate literature are ("blockchain") and produce literature findings as shown in table 2.

TABLE II. RELATED STUDY FINDING RESULT

Database Journal	Article founds
IEEE	449
Springerlink	22
Scopus	179
ScienceDirect	60
Total	710

Then we applied inclusion and exclusion criteria to select the appropriate candidate for article will be explored further.

TABLE III. INCLUSION AND EXCLUSION CRITERIA

Criteria	
Inclusion criteria	<ul style="list-style-type: none"> <li>- Article in peer reviewed paper</li> <li>- Article written in English</li> <li>- Article in open access</li> <li>- The article discusses the use of blockchain technology in current application</li> </ul>
Exclusion criteria	<ul style="list-style-type: none"> <li>- Book</li> <li>- Non-peer reviewed articles, white paper</li> <li>- The article only review blockchain technology</li> </ul>

After applying inclusion and exclusion criteria above, we get 35 appropriate articles that become the main reference in completing the SLR which is published in a periodical journal or international conference proceedings as shown in table 4.

TABLE IV. LIST OF ARTICLE DISTRIBUTION

Publication Media	Sum of Article
Journal Q1	9
Journal Q2	1
Journal Q4	1
Conference Proceeding	24
Total	35

The last step done in SLR is to synthesize and explain the results as described in section 3

### III. RESEARCH RESULT

This section explains each research question defined in section 2, namely: blockchain technology and blockchain implementation.

#### A. Blockchain Technology

Blockchain is one technology that does not use third parties in a data exchange process which in this case occurs in the transaction process. Simply put, if you buy something in the shop by paying using a debit card, the store will believe the balance you entered has already entered their account. Well, the third party referred to here is a bank company which is the liaison of the buyer and seller in the transaction using the debit card.

Many are interested in utilizing blockchain in building information systems. Some components or technologies of blockchain that are utilized in several studies are smart contracts, distributed systems, and cryptography.

##### A.1 Smart Contract

A Smart Contract is a code about the condition of a transaction that can execute itself, stored on the blockchain, which is not controlled by anyone or a third party and therefore everyone can trust. Smart contracts that can be executed on the blockchain can be self-defined according to needs. as well as when writing code, rules, objects, data models, defined, the contract can then begin. After the smart contract is executed, they cannot be stopped or separated from the blockchain, and people can see whether the results of the smart contract implementation are correct or not[1].

In the use of smart contracts, basic ethereum smart contracts are preferred over smart bitcoin contracts. That's because, while Bitcoin smart contracts are only intended to validate currency transactions, the Ethereum network provides various use cases, with the ability of the smart contract[1][2].

##### A.2 Distributed System

Blockchain is a distributed database, which sequentially stores a chain of data packaged into locked blocks [4] in a safe and unchanging way[3]. Blockchain is a distributed database, which sequentially stores a chain of data packaged into locked blocks [4] in a safe and unchanging way. there are two things that must be determined in the distributed blockchain system, including distributed consensus and network nodes.

##### A.2.1 Distributed Consensus

Because blockchain is a distributed database that relies on a P2P network, each node from the network stores a copy of the valid ledger status and the unvalidated data set that needs to be entered into a new block and added to the ledger. In order for the blockchain network to continue to function, nodes need to agree on certain conditions of the ledger contents and on how to package data into blocks. This is achieved by a distributed consensus protocol, which validates the sequential sequence of data generated. The distributed consensus protocol ensures that the quorum blockchain network node agrees on the state of the block from the shared ledger, so that the order in which new blocks are added to the ledger. Following are the distributed consensus algorithms that are often used including Proof-of-Stake (PoS), Proof-of-Work (PoW), proof-of-importance, Delegate Proof-of-Stake (DPoS), proof-of-burn, proof-of-activity, proof-of-deposit.

##### A.2.2 Network Nodes

To have a fully functional blockchain network, a set of network nodes is needed, which is the backbone of the blockchain. Because a blockchain network is a type of P2P

network, a node can be considered as a peer when it starts to connect and communicate with other nodes in the network, so the right name will become a peer-node. For the sake of convenience, we will then mark it as a node. Technically, the blockchain node is a computer that has the core blockchain client installed and operates a complete copy of the blockchain ledger.

Furthermore, the utilization of technology will be classified in 3 parts, namely smart contracts, distributed systems and cryptography. The results of the classification of the discussions in the reviewed paper are listed in table v.

TABLE V. BLOCKCHAIN TECHNOLOGY

No	Technology	Reference
1	Smart Contract	[1], [2], [4], [5], [6], [7], [8], [9], [10], [11], [12], [13], [14], [15], [16]
2	Peer to peer blockchain Network / Distributed system	[3], [17], [4], [18], [19], [5], [20], [21], [22], [23], [24], [11], [12], [25], [26], [14], [27], [15]
3	Blockchain authentication / Blockchain Cryptography	[28], [19], [5], [29], [10], [23], [26], [14], [27], [15], [30]

The technology classification above does not mean that the development of the system that is carried out does not involve other parts of the blockchain technology still more to the part discussed specifically while the other parts do not.

The types of research that usually focus on smart contracts according to the existing review are those that emphasize how data integrity can be maintained. Besides that, the discussion also covers the distribution of the results of a work process. On the other hand, development / research that focuses on distributed systems usually has a problem of how best to share resource needs that were previously centralized and very large to be distributed and not too large. while for research that focuses on cryptographic research subjects discussed are related to the authentication process and how to ensure data integrity related to the hashing process.

#### B. Blockchain Implementation

In general, blockchain provides several benefits when applied in a business process. First, its decentralized nature can expand financial access because there are no limited intermediaries in the transaction process. This at the same time presents efficiency because there is no time and place limit in its operations.

Second, creating financial solutions with lower transaction costs - if compared to conventional transaction rates - while maintaining transaction security. The nature of cryptocurrencies which are composed of complicated (encrypted) algorithms and validated by networks that carry blockchain is considered very safe. With these advantages, it is expected that the banking business will become the most disrupted blockchain, despite the limited real application. then the blockchain implementation classification will be divided into several parts, namely financial (cryptocurrency) and non-financial (Power / Electricity, Security, Internet

Application, decentralize storage, Decentralize IoT, Education, Decentralize Application) categorization of paper review results into the implementation field are listed in table vi

TABLE VI. BLOCKCHAIN IMPLEMENTATION

Type	Application	Reference
Financial application	Crypto-currencies	[30]
Non-financial application	Power / Electricity	[2], [19], [20], [11]
	Security	[6], [31], [7], [21], [27]
	Internet Application	[1], [22], [8], [10], [15]
	Decentralize Storage	[17], [22]
	Decentralize IoT	[4], [23], [24], [25], [13]
	Education	[3]
	Decentralize Application	[18], [5], [32], [29], [26]

From the results of the table classification above it can be seen that the use of blockchain technology is widespread from the financial system to non-financial. Likewise, in the non-financial system the system is also divided very widely from the field of information system security to education.

because there is a need to see more detail about blockchain utilization in the security field. the next process is to classify the implementation of security fields into aspects / fields including confidentiality, integrity, availability, digital forensic, authentication. The classification results can be seen in table vii.

From the table vii can be seen if the use of blockchain in system security also varies. There is blockchain usage in ensuring confidentiality and authenticity, and there is the use of blockchain to prepare the system for digital forensic. In the paper review process, so far no one has discussed / examined the use of blockchain for systems that ensure availability and integrity.

TABLE VII. BLOCKCHAIN IMPLEMENTATION IN SECURITY

Type	Sub-Type	Reference
Security	Confidentiality	[6]
	Integrity	-
	Availability	-
	Digital Forensic	[31], [7], [21]
	Authentication	[6], [27]

## IV. CONCLUSION AND FUTURE WORK

The use of blockchain technology is growing. Research to develop systems that adopt blockchain technology is increasing. Various applications have been developed by adopting blockchain technology. The use of blockchain technology is not limited to financial aspects but also to all types of applications / implementations. This makes sense because all systems need technology to ensure their systems are safe, have integrity with resources that are not too large.

Blockchain technology adopted by researchers and developed in their systems is divided into 3 parts, namely smart contract, distributed system, cryptography. While the

implementation of blockchain in the current system is divided into financial and non-financial.

So the use of blockchain technology is not only limited to cryptocurrency, there are many who use it for other business processes (non-cryptocurrency).

The challenge ahead is how to conduct feasibility studies in certain fields (Digital Forensic Readiness) in adopting blockchain technology

## REFERENCES

- [1] A. K. Koç, E. Yavuz, and G. Dalkılıç, "Towards Secure E - Voting Using Ethereum Blockchain," 2018.
- [2] L. Thomas, C. Long, P. Burnap, J. Wu, and N. Jenkins, "Automation of the supplier role in the GB power system using blockchain-based smart contracts," *CIRED - Open Access Proc. J.*, vol. 2017, no. 1, pp. 2619–2623, 2017.
- [3] M. Turkanović, M. Hölbl, K. Košič, M. Heričko, and A. Kamišalić, "EduCTX: A blockchain-based higher education credit platform," *IEEE Access*, vol. 6, no. March, pp. 5112–5127, 2018.
- [4] O. Novo, "Blockchain Meets IoT: An Architecture for Scalable Access Management in IoT," *IEEE Internet Things J.*, vol. 5, no. 2, pp. 1184–1195, 2018.
- [5] J. Gao *et al.*, "GridMonitoring: Secured Sovereign Blockchain Based Monitoring on Smart Grid," *IEEE Access*, vol. 6, pp. 9917–9925, 2018.
- [6] X. Huang, C. Xu, P. Wang, and H. Liu, "LNSC: A Security Model for Electric Vehicle and Charging Pile Management Based on Blockchain Ecosystem," *IEEE Access*, vol. 6, pp. 13565–13574, 2018.
- [7] M. Hossain, R. Hasan, and S. Zawoad, "Probe-IoT: A public digital ledger based forensic investigation framework for IoT," *IEEE INFOCOM 2018 - IEEE Conf. Comput. Commun. Work. (INFOCOM WKSHPS)*, pp. 1–2, 2018.
- [8] L. Kan, Y. Wei, A. Hafiz Muhammad, W. Siyuan, G. Linchao, and H. Kai, "A Multiple Blockchains Architecture on Inter-Blockchain Communication," *Proc. - 2018 IEEE 18th Int. Conf. Softw. Qual. Reliab. Secur. Companion, QRS-C 2018*, pp. 139–145, 2018.
- [9] P. D. S, K. Singi, V. Kaulgud, and S. Podder, "Evaluating complexity and digitizability of regulations and contracts for a blockchain application design," *Proc. 1st Int. Work. Emerg. Trends Softw. Eng. Blockchain - WETSEB '18*, no. 1, pp. 25–29, 2018.
- [10] F. P. Hjalmarsson, G. K. Hreiarsson, M. Hamdaqa, and G. Hjalmysson, "Blockchain-Based E-Voting System," *2018 IEEE 11th Int. Conf. Cloud Comput.*, pp. 983–986, 2018.
- [11] G. Kim, J. Park, and J. Ryoo, "A Study on Utilization of Blockchain for Electricity Trading in Microgrid," *Proc. - 2018 IEEE Int. Conf. Big Data Smart Comput. BigComp 2018*, pp. 743–746, 2018.
- [12] L. Y. Yeh, P. J. Lu, and J. W. Hu, "NCHC Blockchain Construction Platform (NBCP): Rapidly Constructing Blockchain Nodes around Taiwan," *Proc. ACM/IEEE Jt. Conf. Digit. Libr.*, pp. 2–3, 2017.
- [13] J. Ellul and G. J. Pace, "AlkylVM: A Virtual Machine for Smart Contract Blockchain Connected Internet of Things," *2018 9th IFIP Int. Conf. New Technol. Mobil. Secur. NTMS 2018 - Proc.*, vol. 2018–Janua, pp. 1–4, 2018.
- [14] D. Ulybyshев *et al.*, "(WIP) Blockhub: Blockchain-Based Software Development System for Untrusted Environments," *2018 IEEE 11th Int. Conf. Cloud Comput.*, pp. 582–585, 2018.
- [15] P. Tasatanattakool and C. Techapanupreeda, "Blockchain: Challenges and applications," *Int. Conf. Inf. Netw.*, vol. 2018–Janua, pp. 473–475, 2018.
- [16] J. Wang, M. Li, Y. He, H. Li, K. Xiao, and C. Wang, "A Blockchain Based Privacy-Preserving Incentive Mechanism in Crowdsensing Applications," *IEEE Access*, vol. 6, pp. 17545–17556, 2018.
- [17] M. Dai, S. Zhang, H. Wang, and S. Jin, "A Low Storage Room Requirement Framework for Distributed Ledger in Blockchain," *IEEE Access*, vol. 6, no. c, pp. 22970–22975, 2018.
- [18] J. Gu, B. Sun, X. Du, J. Wang, Y. Zhuang, and Z. Wang, "Consortium blockchain-based malware detection in mobile devices," *IEEE Access*, vol. 6, pp. 12118–12128, 2018.
- [19] G. Liang, S. R. Weller, F. Luo, J. Zhao, and Z. Y. Dong, "Distributed Blockchain-Based Data Protection Framework for Modern Power Systems against Cyber Attacks," *IEEE Trans. Smart Grid*, vol. 3053, no. c, pp. 1–12, 2018.
- [20] S.-C. Oh, M.-S. Kim, Y. Park, G.-T. Roh, and C.-W. Lee, "Implementation of blockchain-based energy trading system," *Asia Pacific J. Innov. Entrep.*, vol. 11, no. 3, pp. 322–334, 2017.
- [21] M. Hossain, Y. Karim, and R. Hasan, "FIF-IoT : A Forensic Investigation Framework for IoT Using a Public Digital Ledger," *IEEE INFOCOM 2018 - IEEE Conf. Comput. Commun. Work. (INFOCOM WKSHPS)*, pp. 1–2, 2018.
- [22] L. Aniello, R. Baldoni, E. Gaetani, F. Lombardi, A. Margheri, and V. Sassone, "A Prototype Evaluation of a Tamper-Resistant High Performance Blockchain-Based Transaction Log for a Distributed Database," *Proc. - 2017 13th Eur. Dependable Comput. Conf. EDCC 2017*, pp. 151–154, 2017.
- [23] K. R. Özyilmaz and A. Yurdakul, "Integrating low-power IoT devices to a blockchain-based infrastructure," *Proc. Thirteen. ACM Int. Conf. Embed. Softw. 2017 Companion - EMSOFT '17*, pp. 1–2, 2017.
- [24] M. Samaniego and R. Deters, "Blockchain as a Service for IoT," *Proc. - 2016 IEEE Int. Conf. Internet Things; IEEE Green Comput. Commun. IEEE Cyber, Phys. Soc. Comput. IEEE Smart Data, iThings-GreenCom-CPSCoM-Smart Data 2016*, pp. 433–436, 2017.
- [25] R. Han, V. Gramoli, and X. Xu, "Evaluating Blockchains for IoT," *2018 9th IFIP Int. Conf. New Technol. Mobil. Secur. NTMS 2018 - Proc.*, vol. 2018–Janua, pp. 1–5, 2018.
- [26] S. Li, "Application of Blockchain Technology in Smart City Infrastructure," *2018 IEEE Int. Conf. Smart Internet Things*, pp. 276–2766, 2018.
- [27] L. Liu and B. Xu, "Research on information security technology based on blockchain," *2018 3rd IEEE Int. Conf. Cloud Comput. Big Data Anal. ICCCBDA 2018*, pp. 380–384, 2018.
- [28] Q. Lin, H. Yan, Z. Huang, W. Chen, J. Shen, and Y. Tang, "An ID-Based Linearly Homomorphic Signature Scheme and Its Application in Blockchain," *IEEE Access*, vol. 6, no. X, pp. 20632–20640, 2018.

- [29] C. Ehmke, F. Wessling, and C. M. Friedrich, “Proof-of-property: a lightweight and scalable blockchain protocol,” *Int. Work. Emerg. Trends Softw. Eng. Blockchain Proof-of-Property*, no. January, pp. 48–51, 2018.
- [30] X. Liu, W. Wang, D. Niyato, N. Zhao, and P. Wang, “Evolutionary Game for Mining Pool Selection in Blockchain Networks,” *IEEE Wirel. Commun. Lett.*, vol. 2337, no. c, pp. 1–4, 2018.
- [31] L. Van Der Horst, K. K. R. Choo, and N. A. Le-Khac, “Process Memory Investigation of the Bitcoin Clients Electrum and Bitcoin Core,” *IEEE Access*, vol. 5, pp. 22385–22398, 2017.
- [32] J. Lin, Z. Shen, C. Miao, and S. Liu, “Using blockchain to build trusted LoRaWAN sharing server,” *Int. J. Crowd Sci.*, vol. 1, no. 3, pp. 270–280, 2017.