A Survey Blockchain and Smart Contract Technology in Government Agencies

A Survey Blockchain and Smart Contract Technology in Government Agencies

E S Negara[1*], A N Hidyanto[2], R Andryani[1], D Erlansyah[1]
[1]Faculty of Computer Science, Universitas Bina Darma
[2]Faculty of Computer Science, Universitas Indonesia

Email: e.s.negara@binadarma.ac.id

Abstract. The development of Blockchain and Smart Contract technology provides significant changes in the form of solutions to social technology problems, such as the problem of document forgery on e-government services. In its implementation of government services, there are several challenges faced, such as social technology problems, blockchain mechanisms, virtual machines, and smart contract code levels, and automation of disintermediation. This paper summarizes and discusses the methodology and research results from various recent papers on the state of the use of smart contracts in e-government services and the weaknesses and potential problems in the use of e-government services.

1. Introduction

The contribution and implication of implementing blockchain technology is the improvement of data transaction and communication methods in database systems, where the transaction and data communication methods on the blockchain are decentralized and distributed, where each block contains a cryptographic hash to form a network. The advantages of blockchain technology that can deal with problems such as codification, security, privacy, performance, and traceability are the variables that cause the adoption of this technology to become increasingly popular.

The development of blockchain technology has contributed a lot to various sectors such as: transport and logistics, technology, media, telecommunications, and public sector services, including e-government services, see Figure 1[1].

One of the trends in the development of decentralized and distributed database system technology is the development of blockchain technology which has facilitated the birth of smart contracts[1]. Smart contracts are computerized transaction protocols that independently carry out contract terms and aim to bind agreements or agreements between multiple parties[1][2]. The main characteristics of smart contracts are disintermediation and transparency. Smart contracts are claimed to increase the efficiency of commercialization of a product, reduce transaction costs, eliminate legal problems, and avoid anonymous transactions [1].

Figure 1. Blockchain opportunities by industrial sector [1]

Various business organizations continue to actively conduct research on the use of blockchain technology for commercial purposes [1]. Likewise government agencies. Currently, various blockchain technology development projects are continuously being developed. At least more than 100 blockchain technology development projects were carried out in the development of government systems in 30 countries [3]. In Indonesia, this technology is also one of the priorities of national research with the theme of developing systems/platforms based on open source with the topic of information technology systems, e-Government communications, artificial intelligence and data analytics [22].

The rapid development of blockchain technology is due to the fact that this technology is directly related to social organizations. Unlike other technologies with traditional consensus. Blockchain works by a consensus algorithm that is pre-agreed upon and after that cannot be modified or faked [3]. Behind the benefits, there are several challenges related to the issue of technology adoption, security and reliability of blockchain technology. In addition, the adoption of smart contract technology also has challenges in adapting the legal framework in a country. Therefore the main research question is:

RQ 1. What is the state of smart contract utilization in e-government service?

RQ 2. What are the Weaknesses and Potential Problems in utilization in e-government service?

This article will discuss the state of the art blockchain technology and smart contract, reviewing the benefits of using them and the potential problems that can arise from using smart contracts in government agencies.

2. Literature Review

2.1 Blockchain Technology and Smart Contracts

The basic concept of blockchain is a distributed database of public records where all digital transactions are executed and shared with participating parties. Each transaction is verified by the consensus of the majority of participants in the system. Records entered in the blockchain system can never be deleted. One of the popular blockchain products is Bitcoin. Bitcoin is a decentralized peer-to-peer digital currency. In its development, digital currencies such as Bitcoin have met with controversy in both financial and non-financial applications. But blockchain has a strong basis so that the controversy can be controlled [15]. Blockchain has five main characteristics, namely: a decentralized database, peer-to-peer transmission, transparency of encryption, permanent data recording, and digital programming based.

In another article, blockchain is a distributed digital transaction and data management system where all users of the system have one consensus or agreement together [15][16][17]. With a distributed system, blockchain eliminates the role of intermediaries which impact the cost of transacting data which is cheaper and safer from data/information manipulation attacks [18]. The mechanisms that make blockchain safe [19] are: Hashing with fingerprint codes; Proof of work; Distributed P2P network. See Figure 1 which is a Blockchain Chain.

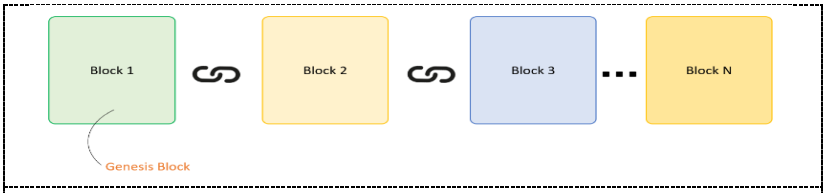

Figure 2. Blockchain chain

Myungsan Jun explained blockchain features with the concept of "social technology" [3]. Social technology is interpreted in a way to communicate, cooperate, compromise, and make agreements between several parties [3]. In addition, social technology also consists of the division of labor, social institutions, and decision-making processes. This technology directly affects the structure of society, systems, social relations, and individual interactions [4].

In its application, physical technology and social technology are related. Where physical technology can praise social technology and allow for the creation of new social technologies. For example, internet technology eliminates geographic boundaries in communicating. Therefore, various studies continue to be conducted to develop social technology based on physical technology interventions. Satoshi Nakamoto's research on blockchain technology is an example of this case [5] [6].

In its development, blockchain technology is expected to change social organizations including the bureaucracy, organizational forms, and the domain of modern society. This is because blockchain is an individual mediation technology and is considered a coercive technique that limits individual activity. Individual mediation is defined as the interaction with each other determined by technology [5] [6].

Bolckhain technology is continuously developed with the concept of automatic algorithm society with artificial intelligence and big data. This technology application is software that can provide logic and control, especially in limiting how individuals behave and interact with this technology. Therefore, Professor Lawrence Lessig formulated the proposition "Code is Law" or "Code as Law" to describe this idea [7].

One of the products of blockchain technology is smart contracts. In particular, the features of a smart contract are considered to have great potential for development. Because smart contracts can set rules and define conditions for contract execution automatically. The advantages of blockchain technology implemented in smart contracts can prevent hacking or contract forgery. So that with this concept it will be possible to build an absolute law [8].

Smart contracts are digital coded containers that encode real-world contract deals. The main element of a contract is an agreement that binds two or more parties. Where each party has obligations based on the agreement. Another element is that the agreement is mediated by a centralized legal entity or can be referred to as a third party. However, with a smart contract, third party functions can be eliminated because both parties already have a digital contract key. Digital contract lock is an automatic code execution that is distributed and verified by a decentralized blockchain network system. Therefore smart contracts are considered as the latest technology that can be trusted to eliminate dependence on third parties and eliminate third party commission fees [9].

Another definition of a smart contract is an autonomous agent. Smart contracts as autonomous agents are stored on the blockchain which are recorded by coding creation transactions then contracts are introduced to the blockchain. Then the smart contract is identified by the contract address. Each smart contract has a sum of virtual coins (Ether), has its own store, and is associated with a predefined executable code. The contract status consists of two main parts: personal storage and the amount of virtual coins (Ether) which is referred to as balance [20].

Smart contracts are developed on top of the cryptocurrency platform. Cryptocurrency is a decentralized cryptosystem that deals with a shared global ledger in the form of virtual money. Users can transfer money and interact with contracts according to agreements signed via cryptocurrency

network transactions. The network consists of mining nodes in charge of disseminating information, storing data, and updating data. The smart contract scheme is shown in Figure 2 [21].

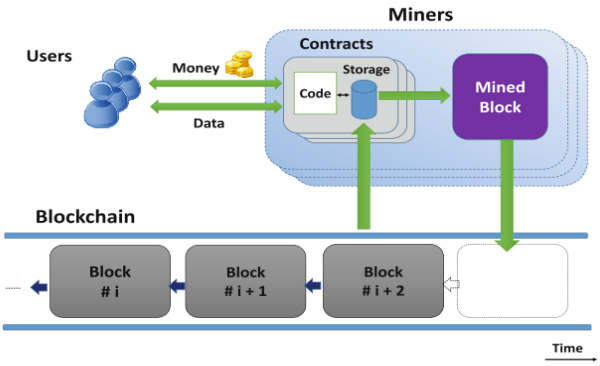

Figure 3. Cryptocurrency Decentralized Scheme on Smart Contracts [21].

Smart contracts consist of the following platforms:

- Ethereum. The biggest and most popular platform for smart contracts is Ethereum. Ethereum smart contracts are utilized in many digital transactions such as building distributed applications, building social networks and identity systems, predicting markets, and various types of financial applications.
- Bitcoin. Bitcoin smart contract technology is a cryptocurrency system that provides new ways to increase the circulation of capital, new markets, and new decentralized autonomous organizations. Bitcoin uses the OP_RETURN transaction of the bitcoin scripting language to store metadata on the blockchain.

Apart from Bitcoin and Ethereum, some new platforms have emerged from either the original Bitcoin blockchain or standalone and offer new enhancements and approaches to the bottlenecks found in the previous platform.

3. Discussion

3.1 Utilization of Blockchain Technology and Smart Contracts in E-Government Services.

Blockchain technology and smart contracts have been widely used in various projects carried out by governments in various countries. There are at least 17 countries that are undergoing various projects by the government (apart from voting systems and digital currency projects) such as; in the United States (US) the government is developing an online personal health data exchange, in the UK through the Department of Labor and Pensions is testing a welfare payment system that carries the concept of blockchain, and in China is developing an asset storage system with the main base of blockchain technology with capacity of 100 transactions in October 2016, as well as various other projects in several countries that the author believes are still in the planning stages or progress. In addition, there are other uses in government agencies in the form of blockchain-based electronic voting system projects, and blockchain-based digital currency projects around the world [3].

The systematic literature review conducted by Yli-huumo et al summarizes the general concept of blockchain technology that has been developed by various researchers [10]. The study shows that 80% of bitcoin development projects focus on security and privacy themes. And since 2016 blockhain applications have diversified. Therefore Yli-huumo et al conducted a research that focuses on cybersecurity and blockchain applications [10].

Meanwhile, at the end of 2016 Conoscenti et al also conducted a systematic literature review on the use and adaptability of blockchain, especially to the Internet of Things (IoT) and several other peer-to-peer devices [11]. The results of these studies show that blockchain can be used for data misuse detection without the need for a central reporting mechanism [11]. A literature review was also carried out by Seebacher and Schüritz [12]. The results of his study show the blockchain service system plays an integral role in facilitating shared value creation, ensuring the availability of information and providing a system coordination mechanism [12].

According to research conducted by Myungsan Jun [3], what makes many countries start blockchain projects is because it is different from other traditional technologies where the consensus mechanism is not a machine but a human domain, blockchain technology works with a human consensus algorithm that functions to decide what data is considered genuine. then stored on the blockchain. This technology allows all parties to validate the data and save the original verified version. Verified data cannot be changed or falsified.

The other main benefits of implementing blockchain technology in government are claimed to be as follows [13]:

- Reducing the economic costs, time, and complexity of exchanging information between government and public-private which improves the functioning of government administration.
- Eliminate bureaucratic channels, eliminate discretionary power, and prevent corruption. This is possible because of the use of distributed nested books and short-cut contracts that have been programmed before.
- Can improve the automation, transparency, auditability and accountability of information in government services.
- Can increase trust in organizational governance through the use of smart contract algorithms which are under government control

Thus, blockchain is a state-of-the-art social and physical technology that simultaneously enables a system that is immutable and tamper-resistant, making it optimal in handling public data that cannot be forged. With the smart contract feature, this technology has the potential to replace existing social organizations, making blockchain one of the most innovative digital technologies that can be considered in the new paradigm of government policymaking and service delivery.

3.2 Weaknesses and Potential Problems

After discussing the state of the art regarding the concept of blockchain technology, printar contracts and the use of this technology in government services, this article also discusses the weaknesses and potential problems of smart contract law in the case of technology adoption and adaptation. As is well known, almost all technologies are vulnerable to cyber attack threats. Cybercrime has caused many economic losses, especially losses that occur due to cyber attacks on digital commercial transactions, theft of personal information and digital financial threats. This condition causes the risk of security breaches to continue to increase exponentially [1].

Utilization of smart contracts requires the involvement of each party in the digital transaction contract being carried out. This can threaten the risk of information transaction sensitivity. In addition, hackers have a lot of skills and adaptability to the system today. So that it allows opportunities for threats to system attacks such as blockchain [1]. The increasing intention of cyber crime is partly due to the increasing value of virtual currencies and the increasing use of smart contracts. This condition inspires cyber criminals to steal digital money, ask for ransom and carry out illegal transactions [1].

The results of a systematic mapping study conducted by Macrinici D, et al, which summarizes several studies on smart contracts on blockchain technology that show at least 16 smart contract problems. All of these issues are categorized into three main issues: blockchain mechanisms, virtual machines, and smart contract code level. From the results of the study, the biggest problem is the problem of blockchain mechanism and the source code of smart contracts. This is due to the

complexity of the blockchain, which consists of scalability, security, privacy, and human error invoices. Human error factors include lack of knowledge, programming errors, and typing errors [14].

Another problem that can arise from this technology is related to the main rationale of smart contracts, namely disintermediation automation. This concept is a contract between parties that execute themselves without an intermediary trusted to facilitate transactions or agreements such as non-digital commercial transactions (traditional functions) which are usually mediated by legal persons or financial authorities. The traditional function of financial experts and commercial lawyers today can also be carried out using smart contracts so that they can replace their roles that are usually profitable to become disadvantaged. Some argue that the financial and legal workforce may suffer losses due to unreliable blockchain technology [14]. However, the authors argue that smart contracts will not pose an immediate and serious threat as feared. There will still be room in various sectors for professionals and lawyers who remain deeply embedded in our global economy because they can think in ways that computers cannot.

4. Conclusion

Blockchain is a cutting-edge social and physical techniques that can solve problems that often occur in handling public data such as data falsification. By utilizing the smart contract feature in e-government, this technology can solve existing social problems, so blockchain and smart contracts are among the most innovative digital technologies that can be considered in the new paradigm of government policymaking and service delivery. In implementing and developing smart contract technology for e-government services, apart from social technology problems, there are at least 4 main challenges that may occur, namely the blockchain mechanism, virtual machines, and smart contract code level, and disintermediation automation.

Acknowledgments

Thank you to the Ministry of Research and Technology/National Research and Innovation Agency for research funding assistance through the Post-Doctoral Research scheme in 2020.

References

[1] Mark Giancaspro, Is a ‘smart contract’ really a smart idea? Insights from a legal perspective, Computer Law & Security Review: The International Journal of Technology Law and Practice (2017), doi: 10.1016/j.clsr.2017.05.007. Hal 1-10

[2] Watanabe, H., Fujimura, S., Nakadaira, A., Miyazaki, Y., Akutsu, A., & Kishigami, J. (2016, January). Blockchain contract: Securing a blockchain applied to smart contracts. In 2016 IEEE international conference on consumer electronics (ICCE) (pp. 467-468). IEEE.

[3] Myungsan Jun. Blockchain government - a next form of infrastructure for the twenty-first century. Journal of Open Innovation: Technology, Market, and Complexity. (2018) 4:7. DOI 10.1186/s40852-018-0086-3. Hal 1-12.

[4] Nelson, R.R. & Nelson, K. (2002) “Technology, institutions, and innovation systems”, Research Policy.

[5] Dougherty, D. (2017) ‘Taking advantage of emergence for complex innovation eco-systems’, “Journal of Open Innovation: Technology, Market, and Complexity”, Keynote paper for SOItmC & Riga Technical University 2017 Conference. https://doi.org/10.1186/s40852-017-0067-y.

[6] Nakamoto, S. (2008) “Bitcoin: A Peer-to-Peer Electronic Cash System”, https://bitcoin.org/bitcoin.pdf

[7] Lessig, L. (2000) “Code: And Other Laws of Cyberspace”, Basic Books.

[8] Tapscott, D.,·Tapscott, A. (2016) “Blockchain Revolution”, Penguin Random House UK.

[9] Swan, M. (2015) “Blockchain: Blueprint for a New Economy”, O’Reilly Media.

[10] J. Yli-Huumo, D. Ko, S. Choi, S. Park, K. Smolander, Where is current research on Blockchain technology? - a systematic review, PLoS One 11 (10) (2016) 127.

[11] M. Conoscenti, A. Vetr, J.C. De Martin, Blockchain for the internet of things: a systematic literature review, in: 2016 IEEE/ACS 13th International Conference of Computer Systems and Applications (AICCSA), 2016, p. 16.
[12] S. Seebacher, R. Schritz, Blockchain technology as an enabler of service systems: a structured literature review, in: Exploring Services Science, 2017, p. 1223.
[13] David Allessie, Maciej Sobolewski, Lorenzino Vaccari. Blockchain for digital government, An assessment of pioneering implementations in public services. Publications Office of the European Union, Luxembourg, 2019, ISBN 978-92-76-00581-0, doi:10.2760/942739, JRC115049
[14] Macrinici, D., Cartofeanu, C., Gao, S., Smart contract Applications within Blockchain Technology: A Systematic Mapping Study, Telematics, and Informatics (2018), doi: https://doi.org/10.1016/j.tele.2018.10.004.
[15] Crosby, M., Pattanayak, P., Verma, S., & Kalyanaraman, V. (2016). Blockchain technology: Beyond bitcoin. Applied Innovation, 2(6-10), 71.
[16] Iansiti, M., & Lakhani, K. R. (2017). The truth about blockchain. Harvard Business Review, 95(1), 118-127.
[17] Yli-Huumo, J., Ko, D., Choi, S., Park, S., & Smolander, K. (2016). Where is current research on blockchain technology?—a systematic review. PloS one, 11(10), e0163477.
[18] Xu, J. J. (2016). Are blockchains immune to all malicious attacks?. Financial Innovation, 2(1), 25.
[19] Husni(2019). Mengenal blockchain: Teknologi dibelakang Bitcoin. Komputasi. 3(1).
[20] Luu, L., Chu, D. H., Olickel, H., Saxena, P., & Hobor, A. (2016, October). Making smart contracts smarter. In Proceedings of the 2016 ACM SIGSAC conference on computer and communications security (pp. 254-269). ACM.
[21] Delmolino, K., Arnett, M., Kosba, A., Miller, A., & Shi, E. (2016, February). Step by step towards creating a safe smart contract: Lessons and insights from a cryptocurrency lab. International Conference on Financial Cryptography and Data Security (pp. 79-94). Springer, Berlin, Heidelberg.
[22] Negara, ES., Kerami, D., Wiryana, IM., & Maulana Kusuma TB (2017). Researchgate data analysis to measure the strength of Indonesian research. Far East Journal of Electronics and Communications, 2017, 17(5), pp. 1177–1183.