

The Applicability Blockchain in Indonesia Based on Indonesian Data Privacy Regulation

Q Fadlan¹, Mohammad Achmad Amin Soetomo¹, Bagus Mahawan¹

¹ Department of Information Technology, Swiss German University, Tangerang 15143, Indonesia

Abstract. Blockchain is a distributed ledger technology that has reliability in terms of maintaining data integrity and availability but not data privacy. Therefore, implementation of this particular unregulated technology must be reviewed to ensure compliance with relevant regulations, especially data privacy regulations which is this research main topic. For this reason, implementation of blockchain was observed in comparison with existing data privacy regulations in Indonesia. As initiation steps of research, data privacy regulations from Indonesia, Japan and Europe was used to be the input for the analysis of blockchain implementation. Two additional instruments, questionnaire and interview was used to produce an enhanced design for implementation of blockchain scheme in Indonesia. After the research was done, it was concluded that there is a possibility of blockchain implementation in Indonesia as long as the design was used with some notes as consideration.

Keyword: regulation, blockchain, data privacy, Indonesia, implementation

1. Introduction

Bitcoin as one of the cryptocurrency products is the result of the development of the public blockchain created by Satoshi Nakamoto (Nakamoto, 2008). The main purpose of this development is to reduce and eliminate third parties in the payment system. This deduction uses the context of decentralization and consensus. Where decentralization is a concept used to verify a transaction (Wright and Filippi, 2015). While consensus is the method used to validate transactions (Seibold and Samman, 2016). With these two things, bitcoin is a product that has high integrity and availability.

Seeing the advantages of the blockchain, blockchain is still in the development phase in addition to the financial industry (cryptocurrency). Industries such as logistics, healthcare and banks have the potential to utilize blockchain (Lewis, 2015). However, there are some things that are still an obstacle in blockchain implementation, especially in the data processing process (Halpin and Piekarska, 2017). Permissionless blockchain as a public network allows various types of entities both personal and institutional to join the blockchain network. Considering this is a public network, every data transaction can be seen by all entities in the network. While in some industries, transaction data is data privacy that is very confidential. This makes one of the other concerns of the slow adoption of blockchain by businesses today (Lukacs, 2017).

Given the importance of data privacy, some regions have issued strict rules for the use of data privacy. GDPR is a regulation that regulates European privacy data. While APPI is a regulation established by the Japanese government in conducting privacy data safeguards. Referring to the problems above, Japan is currently developing blockchain based on these regulations (Ministry of Economy, 2017).

The development of blockchain was also felt in Indonesia. Currently the adoption of blockchain in Indonesia has experienced a significant development. However, currently blockchain development is still in the phase of measuring benefits and risks that will occur in blockchain adoption (Probank, 2017). In maintaining the security of data privacy of Indonesian society, the Indonesian government also has regulations governing the data privacy (DLA, 2018).

The regulation is also have specifically regulated the protection of data privacy on electronic systems. However, there are no studies related to blockchain in Indonesia according to data privacy regulation. Based on the literature that was found during research, one of examples that can be used as a reference is the use of cloud computing technology (Nugraha, 2012) because this technology has the potential to manage data privacy so that it is part of data privacy regulation subject. In another study, there is already a blockchain design that has an architecture such as Figure 1 (Latifa *et al.*, 2017). It can be seen that blockchain has the potential to manage data privacy. But, there are several security holes issues that needs more attention as it may have an impact on someone's privacy on the blockchain (Conti *et al.*, 2017). Therefore, there needs to be a study on blockchain implementation where it must comply with data privacy regulations.

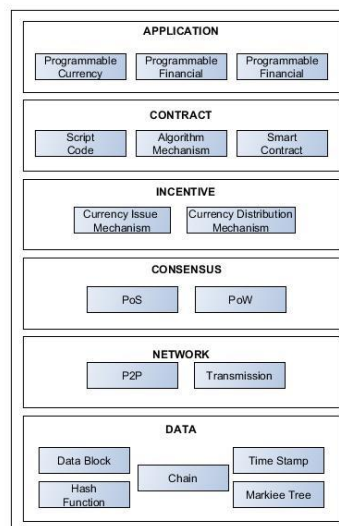


Figure 1.Blockchain Architecture (Latifa *et al.*, 2017)

Referring to the above problems, this paper is intended to assess the potential applicability of blockchain implementation in Indonesia. The main reference is based on the applicable regulations in Indonesia. To support research, GDPR and APPI regulations will be used as additional references. So that hopefully the author can provide recommendations for blockchain architecture design in accordance with data privacy regulation.

2. Methodology

As the objective of this research is to find out about response of Indonesian data privacy regulation for blockchain implementation in order to propose a design that complies with applicable law and regulations, qualitative research was used. These are the procedure that was done during research:

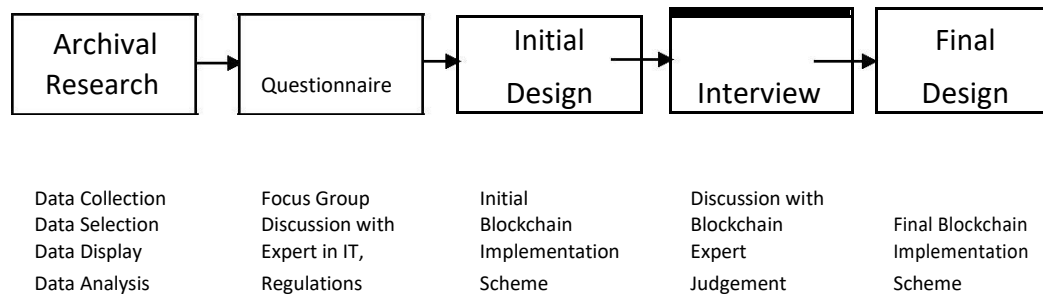


Figure 2. Research Flow

First, archival research that was consist of data collection, data selection, data display and data analysis was done. For data collection, regulation related to data privacy was collected, especially the one in Indonesia. However, regulation of data privacy in Indonesia has not been specifically created but spread over several existing regulations (DLA, 2018). Besides data privacy regulations in Indonesia, there are two more regulations that was collected as part of research. Those are Act of Protection Personal Information (APPI) from Japan which has started to implement blockchain and General Data Protection Regulation (GDPR) from Europe (DLA, 2017) that have broad impact related to personal data processing for Europeans. After the data was collected, it was selected to which relevant with the objective of this research. As a result, relevant Indonesian regulation has been grouped on Table 1, which is also part of data display.

Table 1. Data Privacy Regulation in Indonesia

No	Law	Number of articles	Note
1	Regulation of the Minister of Communication and Information No. 20 of 2016 on Protection of Personal Data in Electronic Systems.	38	Articles 1 through 38
2	Law Number 19 of 2016 About Amendment To Law Number 11 of 2008 About Information and Electronic Transaction	6	Article 26, Article 30, Article 31 Article 32, Article 33, Article 35
3	Government Regulation No. 82 of 2012 on the Implementation of Electronic Transactions and Systems	2	Article 1 no 27 Article 15
4	Law Number 24 of 2013 regarding Amendment to Law Number 23 of 2006 regarding Population Administration	1	Article 84

After that, the collected data was analyzed to draw initial conclusion as the input for the questionnaire. The data privacy regulation was compared to blockchain mechanism, which leads to criteria that may fulfill the compliance criteria.

Second, questionnaire was used as part of instrument to evaluate the archival research analysis result. In this part, convenience sampling was used and the criteria for the participant of questionnaire is Expert in Security, Privacy and also understand about blockchain. For the questionnaire itself, open ended questionnaire was presented to the participants, so any additional recommendation can be added as part initial design. Third, initial design of framework was composed based on the result of the questionnaire. Forth, interview was done to evaluate the initial design. Different with the first questionnaire, the interview's participant is the expert of the subject itself which in this research is blockchain. By doing this, it was expected that validity can be constructed through triangulation of multiple sources (Yin, 2002). Fifth and the last, final design was composed based on analysis on the interview result. Analysis was done by combining the first and second instrument result.

However, there is a limitation in this research which is the scope. In this research, the main data that was being used is regulation in Indonesia. For the subject itself, the blockchain that is referred is the blockchain on bitcoin.

3. Result and Discussion

3.1. Data Privacy Regulation Comparison

As the first step of the research, the author comparing the data privacy regulation among APPI, GDPR and Indonesia. Gap analysis is the main objective of the comparison process as described on table 2.

Table 2. Data Privacy Regulation Comparison

No	Parameter	Indonesia	Japan	Europe
1	Objective	Protect data privacy on Information and electronic transaction	- Protect personal data - Support business to growth	Protect personal data
2	Definition Personal Data	data that can identify individuals, directly and indirectly	data that can identify individuals, directly and indirectly	data that can identify individuals, directly and indirectly
3	Collecting and Processing	inform the purpose of data collection and processing	inform the purpose of data collection and processing	inform the purpose of data collection and processing
4	Data Controller	Electronic system organizer	Business operator	Data Controller
5	Data Correction	Not yet clearly regulated the procedure for deleting personal data	provide an optional mechanism to delete privacy data	Owner of data must remove directly the data

Defining the data privacy terminology, author used five parameters to analyze the regulations. According to the data, three regulation described the same definition and characteristic of data privacy. However, there is a very significant difference in the context of data correction. GDPR will regulate data privacy is tighter than the other two regulations. While the rules in Indonesia there is no regulation that states explicitly how to treat the data correction.

3.2. Implementation blockchain in Japan

Japan is success story of blockchain Proof of Concept. The story can be summarized on table 4. It has been tested for vary industries especially for Banking industry. For other industry, BitFlyer workin closely with the other companies such as Hitachi, Fujitsu and NTT Data to develop Miyabi Blockchain.

Table 3. Result of Blockchain's PoC

No	Proof of Concept	Result
1	Establishment of future backbone operation systems that utilize blockchain technology	Successfully conduct transaction for 2,5 million account with capacity 90.000 per hour (Daisuke Yamazaki, 2016)
2	Streamlining cross-border settlement processes in securities transactions	Reduce time for cross-border transaction from 3 days to 1 days and information can't be tampered (Mizuho Bank, Ltd.,Fujitsu Limited, 2016)

3	Japanese Domestic Interbank Payment Operation	Reduce cost for interbank transaction (Deloit, 2016)
4	Applicability of Distributed Ledger Technology to Capital Market Infrastructure	Identify potential and limitation of the DLT application to capital market infrastructure (Santo <i>et al.</i> , 2016)
5	Biometrics Verification System for Retail	Implement Coupon system based on Biometric data. Biometric data of customer stored on Blockchain. The result are reduce of verification time and easu registration and authentication. (Hitachi, 2018)
6	Blockchain Supply Chain	Improve efficiency of procurement and inventory management (Hitachi, 2017)

The proof of concept has involved three major blockchain. Miyabi is the biggest while Iroha Hyperledger and Hyperledger Fabric are the other blockchain technology is involved for the PoC. Table 5 show the blockchain comparison used for Proof of Concept.

Table 4. Blockchain PoC comparison

	Miyabi	Hyperledger Iroha	Hyperledger Fabric
Consensus	BFK2	YAC	Pluggable
Type of Blockchain	Permissioned	Permissioned	Permissioned
Company	BitFlayer	Soramitsu	IBM
License	Enterprise	Open Source	Open Source
Objective Blockchain	Fast Transaction	Development Application	Complexity and Confidentiality

Referring to the table 3, all the blockchain type is the permissioned blockchain. The character of this type can be summarized as follow:

1. There is a selection and verification process to join the blockchain network
2. Not everyone can join and get existing data on the blockchain
3. There must be one party in charge of regulating and monitoring the blockchain network

3.3. Blockchain and Indonesian Data Privacy Regulation

As the developed country, Indonesia's government has several regulations to control the data privacy. The data privacy is considered as part of the customer data. The protection will refer to separate regulation, as follows:

1. Law number 11 of 2008 on Electronic Information and Transactions (EIT Law). It has been amended in 2016 for regulation number 19 and it is implicitly discussed of a data or electronic information, both general and personal (Government, 2008).
2. Government Regulation No. 82 of 2012. on the implementation of electronic systems and transactions for personal electronic data (Government, 2012).
3. Regulation of the Minister of Communication and Information No. 20 of 2016 concerning the protection of personal data in electronic systems (Information, 2016).
4. Law Number 24 of 2013 Article 84. It describes the protection of Indonesian citizens personal data (Government, 2013).

Table 5. Blockchain and Indonesia Data Privacy Regulation

No	Regulation	Data Privacy Parameter	Blockchain
1	Minister of Communication and Information No. 20 of 2016 article 1	Data personal confidentiality	Decentralized network addresses the data among the node. It is potentially every connected node can easily read the transaction data.
2	Law No. 11 of 2008 Article 16		
3	Minister of communication and information number 20 of 2016 article 1 point 2	Personal data is the data attached to the person whether it is directly recognizable or indirectly	Blockchain address pseudonym which allows to reveal the identity of the individual, then this will also violate the provisions of the privacy data protection regulations
4	Law Number 24 of 2013 Article 84	Personal data that must be protected	Since the data stored on the blockchain can be accessed by all members of the blockchain then when blockchain is implemented in other sectors, these data must be protected

3.4 Blockchain Design for Data Privacy Regulation

According to the data privacy regulation and compared to the blockchain capabilities, the table 6 shows the blockchain comparison among regulation.

Table 6. Regulation response for blockchain's recommendation to protect data privacy

No	Recommendation for Blockchain	Indonesia	Japan	Europe
1	There is one organization that complies with the laws that are responsible for the blockchain network	OK	OK	OK
2	Filter and Selection member of blockchain	OK	OK	OK
3	Private network for blockchain	OK	OK	OK
4	Encrypt data on blockchain	OK	OK	OK
5	Using another option for remove data on blockchain	OK	OK	NO

From the regulation perspective, GDPR article number 17 stated that the privacy data must able to be removed on any application, including the blockchain. Meanwhile the Indonesia and APPI is less restrict, data privacy disposal can be treated as the optional part. Regulation will accept if the developer has the mitigation process to control or remove it.

Based on the data privacy regulation, the successfully blockchain implementation must to be follow the recommendation as follow:

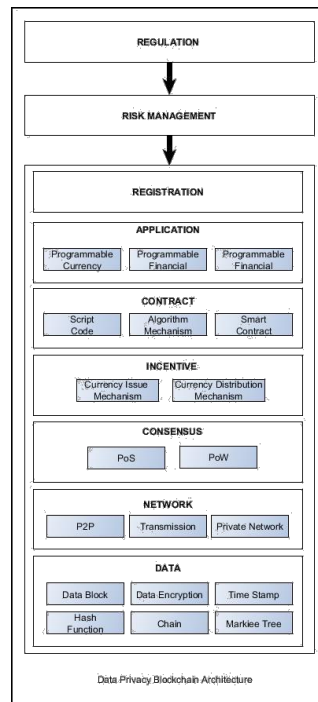


Figure 3. Blockchain design for data privacy regulation

1. Governance process. This will regulate and monitor any rules that applicable to the blockchain network. It will be including of data privacy determination must be maintained.
2. Registration. The registration will control the parties who are trying to join the blockchain network known as the permissioned blockchain. This will address the responsible control to the parties.
3. Private Network. This part will prevent the blockchain from the cyber-security attack due to only certain parties who has key will be involved in transaction.
4. Encryption Data. Securing process has to be covered into data level. Thus, the encryption must be applied for every single data. Only authorized party will able to read the data (Deloit, 2016).

4. Conclusion

Referring to the results of the research above, blockchain implementation can be done in Indonesia. However, there are several things that must be adapted to the applicable regulations in Indonesia. One of them is the aspect of data security privacy that is protected by law. For that we need an architecture customization that refers to the applicable regulations, in the form of:

1. Governance process
2. Registration process (permissioned)
3. Private network
4. Data encryption

References

Act on the Protection of Personal Information (APPI) 2016. Available at: https://www.ppc.go.jp/files/pdf/280222_amendedlaw.pdf (Accessed: July 11, 2018).

Conti, M. *et al.* (2017) 'A Survey on Security and Privacy Issues of Bitcoin'. doi: 10.1007/978-3-319-52015-5.

Daisuke Yamazaki (2016) *SBI Sumishin Net Bank succeeds in using blockchain for their mission-critical systems ; using " mijin " by Tech.* Available at: <http://mijin.io/en/599.html> (Accessed: 1 August 2018).

Deloit (2016) *Report on Practical Experiment of Blockchain Technology in Japanese Domestic Interbank Payment Operation*. Available at: <https://www2.deloitte.com/content/dam/Deloitte/jp/Documents/about-deloitte/news-releases/jp-nr-nr20161130-report-en.pdf>.

DLA (2018) *DATA PROTECTION Indonesia*.

Government, I. (2008) *ACT OF THE REPUBLIC OF INDONESIA NUMBER 11 OF 2008*.

Government, I. (2012) *GOVERNMENT REGULATION OF THE REPUBLIC OF INDONESIA NUMBER 82 OF 2012*.

Government, I. (2013) *ACT OF THE REPUBLIC OF INDONESIA NUMBER 24 OF 2013*.

Halpin, H. and Piekarska, M. (2017) 'Introduction to security and privacy on the blockchain', *Proceedings - 2nd IEEE European Symposium on Security and Privacy Workshops, EuroS and PW 2017*, pp. 1–3. doi: 10.1109/EuroSPW.2017.43.

Hitachi, K. (2018) *KDDI、ブロックチェーンと 体ID 認証による クーポン決済実証を実施*. Available at: <http://www.hitachi.co.jp/New/cnews/month/2018/07/0725.pdf>.

Hitachi, M. (2017) *Hitachi and the Mizuho Financial Group to Begin Proof of Concept Regarding the Utilization of Blockchain Technology in the Supply Chain management*. Available at: <http://www.hitachi.com/New/cnews/month/2017/09/170921c.pdf>.

Information, M. of C. and (2016) *REGULATION OF THE MINISTER OF COMMUNICATION AND INFORMATICS OF THE REPUBLIC OF INDONESIA NUMBER 20 OF 2016*.

Latifa, E.-R. *et al.* (2017) 'Blockchain: Bitcoin Wallet Cryptography Security, Challenges and Countermeasures', *Journal of Internet Banking and Commerce*, 22(3), pp. 1–29. Available at: <http://www.icommercecentral.com/open-access/blockchain-bitcoin-wallet-cryptography-security-challenges-and-countermeasures.pdf> <https://search.proquest.com/docview/1992203656?accountid=29104> http://openurl.wu.ac.at/resolve?url_ver=Z39.88-2004&rft_val_.

Lewis, A. (2015) 'Blockchain Technology Explained', *Blockchain Technologies*, pp. 1–27. doi: 10.15358/0935-0381-2015-4-5-222.

Lukacs, A. (2017) 'What Is Privacy ? the History and Definition of', pp. 256–265. Available at: <http://publicatio.bibl.u-szeged.hu/10794/7/3188699.pdf>.

Ministry of Economy, T. and I. (2017) *Japan 's FinTech Vision*.

Mizuho Bank, Ltd., Fujitsu Limited, F. L. L. (2016) *Mizuho Bank and Fujitsu Trial Blockchain to Streamline Cross - Border Securities Transaction Settlements Blockchain technology greatly reduces time required for settlement post - Details of the Joint Trial*. Available at: <http://www.fujitsu.com/global/about/resources/news/press-releases/2016/0308-01.html> (Accessed: 20 July 2018).

Nakamoto, S. (2008) 'Bitcoin: A Peer-to-Peer Electronic Cash System', *Www.Bitcoin.Org*, p. 9. doi: 10.1007/s10838-008-9062-0.

Nugraha, R. A. (2012) 'Analisis Yuridis Mengenai Perlindungan Data Pribadi dalam Cloud Computing System Ditinjau dari Undang-Undang Informasi Dan Transaksi Elektronik'.

Probank (2017) 'Menimbang Manfaat dan Risiko Blockchain', *Probank*, pp. 3–10.

Santo, A. *et al.* (2016) *Applicability of Distributed Ledger Technology to Capital Market Infrastructure*. Available at: https://www.jpx.co.jp/english/corporate/research-study/working-paper/b5b4pj000000i468-att/E_JPX_working_paper_No15.pdf.

Seibold, S. and Samman, G. (2016) *Consensus Immutable agreement for the Internet of value*, *Kpmg*. doi: 10.4155/EBO.13.392.

Wright, A. and Filippi, P. De (2015) 'Decentralized blockchain technology and the rise of'.

Yin, R. K. (2002). *Case study research: Design and methods*. Thousand Oaks, CA: SAGE Publications.