Journal of Multimedia Information System VOL. 6, NO. 3, September 2019 (pp. 125-130): ISSN 2383-7632(Online)
http://dx.doi.org/10.33851/JMIS.2019.6.3.125

A Study on the Effect of Blockchain on Personal Information Protection

Seong-Kyu (Steve) Kim[1,*]

Abstract

In this paper, Blockchain is mentioned as the next-generation core IT technology. As an immature technology, there are not many practical use cases, but it is expected to be widely applied in various industries such as cryptocurrency, finance, public, etc. to increase efficiency and enable new services that did not exist in the past. Nevertheless, the generalization of blockchain technology is still difficult. In particular, from the viewpoint of personal information protection, GDPR of Europe, etc., is becoming stronger. Considering that the core of the blockchain is the change of information sharing and processing method, it is very important how the blockchain can affect, especially from the viewpoint of privacy, and how the Privacy Act can be applied to the blockchain. However, the discussion on this part also seems to be insufficient. Therefore, in this paper, blockchain By analyzing the implications and implications of technologies and services using them from the perspective of the Privacy Act, we will discuss how the blockchain will be used to prevent leakage of privacy.

Key Words: Blockchain, IoT, Artificial Intelligence, Smart Contract, GDPR.

I. INTRODUCTION

Blockchain is being talked about as the next major IT technology. Although there are not many cases of actual use as immature technology, it is widely applied in various industries such as cryptocurrency, finance, and public sectors to increase efficiency and enable new services that did not exist previously [1-3]. Nevertheless, as to the legal implications of the universalization of blockchain technology, it seems that at least not enough analysis has been made in our country. In particular, considering that the core of blockchain is changes in information sharing and processing methods, it seems important to consider how blockchain can be affected, especially from the point of view of privacy, and how the privacy law can be applied to blockchain, but there is not enough discussion in Korea yet. Therefore, this paper will study technologies and improvement measures to protect personal information protection using the desired blokchain by analyzing the meaning and implications of blockchain technologies and their services from the perspective of the Privacy Act I will also deal with the introduction in Chapter 1. Chapter 2 discusses blockchain and personal information protection, while Chapter 3 shows the final conclusions in Chapter 4 of the technologies and services required when blockchain is connected to personal information. This addresses the paper that incorporates blockchain into the required personal information. And personal information protection becomes very important in Europe's GDPR, the US Privacy Act, and Asia's Privacy Act. Due to the leakage of personal information, there is still leakage of personal information using hacking etc. based on cyber attacks using internet weaknesses such as phishing, pharming, and smishing. Therefore, the proposals were made on the basis of Anonymous, Autonomy, Openness, Programmable, Traceability, Tamper Proof, and Collectively Maine, which are characteristics of blockchain to prevent such Internet authentication.

II. Related Research

This paper has various technologies on blockchain, needs for personal information protection, and problems such as GDPR. It also reviews the concept and characteristics of blockchain and deals with specific personal information utilization situations in open blockchain and specific blockchain services in order to provide specific analysis from the perspective of the Privacy Act [4-6].

Manuscript received September 16, 2019; Revised September 29, 2019; Accepted September 30, 2019. (ID No. JMIS-19M-09-028)
Corresponding Author (*): Seong-Kyu (Steve) Kim, GOB Universal PTE., LTD, Singapore, guitara77@gmail.com.
[1]CEO/Ph.D of GOB Universal PTE., LTD, Singapore.

2.1. Blockchain

Blockchain is a ledger management technology based on distributed computing technology where small data under management is stored in a chain-type, link-based distributed data storage environment created based on the P2P method, so that no one can modify it at random and anyone can see the results of the change. This is essentially a form of distributed data storage technology, designed to prevent arbitrary manipulation by operators of distributed nodes as a list of changes that have been continuously changed on all participating nodes. Blockchain technology is used for most cryptocurrency transactions, including bitcoin. Because the transaction process of cryptocurrency is used for de-centralized electronic books, the server runs on each computer of many users running blockchain software, enabling free trade between individuals without central banks [7-9]. Blockchain can be seen as an agreement convergence algorithm that ensures that data on books stored distributed across each node is always available among large nodes. This capability enables the node to run anonymously, or even involve a poorly connected or even untrusted operator. The node of the cryptocurrency has a partial or full blockchain. This eliminates the need to have a centralized database that systems like PayPal need. Whereas the ordinary book records the exchange of checks, receipts, or promissory notes, blockchain is itself a trading book and is a trade certificate [10]. Bitcoin expresses that it exists in the form of unpaid results of transactions. Transactions in blockchain format will be distributed to blockchain networks through software apps such as Bitcoin wallet apps. The nodes in the blockchain network verify the transaction, then add the deal to their books. And the deal spreads the added books to other nodes in the network. These blockchain also suggest a new paradigm in traditional cryptography [Fig. 1].

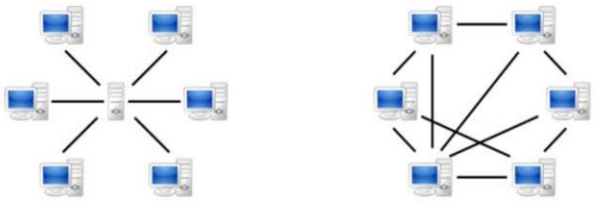

Fig. 1. Peer-to-Peer System for Blockchain.

2.2. Type of Blockchain

Public blockchain is operated through the Internet and is freely available to anyone without the operator's permission to participate in the blockchain network. Anyone can participate in the network by receiving an address (such as a Bitcoin address) for the transaction and downloading and using software to operate the node. That is, anyone can become a blockchain node, add records to the block, and approve transactions. Because of this feature, it is also called "permissionless blockchain" or "unpermitted blockchain." And in a private blockchain or private blockchain, there is a principal who runs the network, and these entities have the authority to decide whether or not to participate in the network of new participants and the relevant rules [Fig. 2]. This is also referred to as a consotium blockchain. As such authority is granted to one principal or institution, aspects similar to traditional centralized methods are also found, such as rule changes or modifications to existing records. In other words, it is likely that these entities are almost equivalent to TTP (the Privacy Act). Finally, semi-public blockchain (converged blockchain) is a combination of open and private blockchain, in which participation in the network is controlled by a free-flow or some pre-selected participants [11-13].

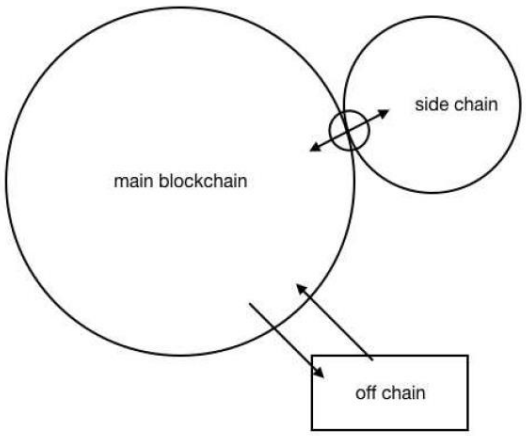

Fig. 2. Type of Blockchain.

2.3. Privacy

Information on living individuals, such as names, resident registration numbers, and videos, can be easily combined with other information, even if it is not possible to recognize a particular individual. And personal information is information about identified or identifiable surviving individuals and takes the basic principles of OECD privacy [14-17]. This includes identifying an individual easily combined with other information, even though the information alone does not identify the individual. And the concept and scope of personal information brings about the diversification of the types of personal information that should be protected by continuously expanding information and communication technology development in accordance with the social environment and technology development of technology [Fig. 3].

1. In case there is only a name: As there are people with the same name, the name alone cannot identify a particular individual, so it does not belong to personal information.
2. Statement+Address: Not only the name but also the address can be added to identify a specific individual, so it is appropriate for personal information.
3. Personal identification number: This information is unique and can identify specific individuals, so it is relevant to personal information.
4. Academic background, experience, and degree of property: This information makes an individual assess and judge, so it is relevant to personal information.

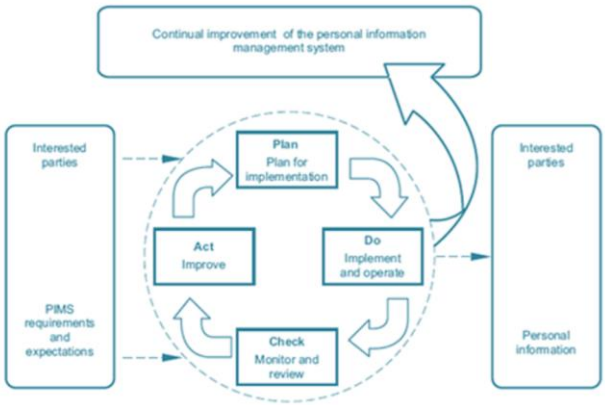

Fig. **3**. Privacy Process.

III. Analysis of the flow of personal information related to blockchain

In the most circular form of a blockchain, all transaction information associated with such a public key, as well as a party to the transaction, is stored on individual nodes that form a blockchain network in the form of a block. In this case, the information that makes the person identify itself is not stored in the block in principle. In addition, no other centralized server processing unit exists to store and control information. In addition, there is no single entity that makes decisions on important matters concerning processing, such as the purpose and means of processing, and controls them. This is because these decisions are made by consensus algorithms already established in blockchain networks and are implemented at the individual node level. This is the basic picture of an open blockchain, in which anyone can participate in a blockchain network. Thus, people in many countries can be blockchain nodes. This also enables the transmission and exchange of information between countries within blockchain.

Public blockchain is the most faithful blockchain to the basic concept of distributed ledger. As such, it is more like a prototype of a blockchain. As mentioned earlier, the key to blockchain is to process transaction-related information without the presence of a third party, a centralized information processor, and to ensure the reliability of the transaction. And by doing so, the philosophical foundation of blockchain is to ensure anonymity of individuals involved in the transaction and to strengthen their authority over information.The Privacy Act also aims to protect individuals and strengthen their authority.

The Book is in line with these blockchain ideals. In particular, the right to self-determination of personal information, which is the constitutional basis of the nation's Personal Information Protection Act, is defined as "the right of the information subject to decide on its own when and to whom and to which extent the information about itself is known and used, i.e. the right of the information subject to decide on its own regarding the disclosure and use of personal information." In this regard, blockchain and privacy laws share their philosophy [18-22].

On the other hand, however, there is room for thinking that the privacy law does not have a single or specific 'personal information processor' in place of the situation in which blockchain and distributed principal technologies have not been popularized, and that nodes that participate in blockchain networks jointly manage information, and that the system of privacy law does not fit together [23-27].

Public blockchain is the area where potential tension between blockchain technology and privacy laws is most clearly shown. In the case of a private (private) blockchain, only a given node that is allowed to participate by a central administrator on a closed network can handle personal information, which is more consistent with the existing privacy law system that has been passed on to a particular person-handler, but in the case of an open blockchain, an unspecified number of nodes can participate, and no central administrator exists. As mentioned earlier, the most common open block chains are virtual currencies such as bitcoin and ether Leeum. This paper vomits around these open block chains. In this regard, however, attention needs to be paid to the following two points.

3.1. Chain ID

The first collection of personal information included in the blockchain for the chain ID service would constitute the collection of personal information. This is done during the process in which users request the issuance of certificates through individual participants. The person who collects the personal information will then be the appropriate participant in the task of issuing the certificate. In addition, the information is automatically shared among each node (participants) in the process of creating a new block

containing personal information, which can constitute a third party provision of personal information under the ICT Network Act. The provision of personal information means the transfer of control and control of personal information to third parties other than the personal information processors. In other words, "supplies" include not only the delivery of personal information, but also the sharing of personal information by allowing access to the DB system, allowing access to it, and by enabling copying. In particular, 'supplies' differ from 'personal information processing consignment' in that personal information is transferred for the purpose and benefit of processing the work of the recipient. Participants in the position of the information and communication service provider in relation to the chain ID service shall destroy the information on blockchain when the user has an obligation to exercise the right to delete or destroy personal information in accordance with law by withdrawing their consent to collect and use personal information or to provide personal information to third parties. However, there is a problem with blockchain information that is not easy to delete. The reliability of data in a blockchain is based on indelible immutability, which is cited as an advantage in ensuring the integrity of the data, but the problem is that it is almost impossible to change or delete the data recorded on the blockchain from the perspective of the Privacy Act. as a solution, consider tying all existing data before a particular destruction point into a single block, processing and destroying the hash function. It would not be possible to rule out the possibility that existing data would be treated as permanently deleted in a non-renewable way if the existing blocks were grouped together to disable them and then a new blockchain would be started after the demolition. However, the unclear interpretation of the technical standards and statutes in this part is as discussed earlier.

3.2. Blockchain and GDPR

The principles of data protection should apply to any information concerning an identified or identifiable natural person. Personal data which have undergone pseudonymisation, which could be attributed to a natural person by the use of additional information should be considered to be information on an identifiable natural person. To determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly. To ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments. The principles of data protection should therefore not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable. This Regulation does not therefore concern the processing of such anonymous information, including for statistical or research purposes.

As above, the GDPR considers all measures likely to be used reasonably by the controller or another person to determine whether personal information is 'identifiable' but considers all objective factors such as cost, time and available technology. In addition, the expert 26 mentions aliased information 131 and anonymous information, which is described as identifiable information and personal information by the use of additional information, and that anonymous information is not applicable to the Act as information not related to identified or identifiable natural persons. As we saw earlier, within the block, an individual's public key is stored as metadata for transaction information, which seems to be personal information, in that it can be seen as an individual when combined with additional information called a corresponding secret key. As we discussed earlier, the exchange has additional information that enables individual identification, so for the exchange, the information stored within the block may be personal information, but there may be problems with the general node.

IV. CONCLUSION

If the information on the public blockchain can be personal, it may contain the personal information of EU citizens, and some of the nodes may be located within the European Union. Then all the nodes in the European Union can be exploited by the GDPR. Does the node handling the personal information of EU citizens subject to GDPR even if it is not located within the EU? In this respect, the GDPR sets forth explicit provisions for the geographical coverage, unlike our Privacy Act. According to this, nodes within the European Union will be subject to the GDPR once they are in the EU. However, even nodes that are not within the European Union are subject to GDPR if they provide goods or services to information entities within the European Union or monitor the behavior of such information entities within the European Union. First of all, the open blockchain node is responsible for maintaining and managing the transaction ledger so that the blockchain transaction can take place, so this may be considered to be a kind of service provision. However, it should be acknowledged that for GDPR, the fact that the controller is simply not sufficient

to provide services to the information entity within the European Union and is clearly expected to provide services to the information entity within the European Union. No literature has been found to have a definitive conclusion on this part. However, this should be assessed on a case-by-case basis, and there is a view that in view of the wider interpretation of Article 3 above, the GDPR is likely to be applied to transactions that are not relevant to the EU. There are numerous difficulties in deciding whether to apply the Personal Information Protection Act to an open block chain and in how the Personal Information Protection Act should be applied. It is thought that a practical solution to such difficulties will be possible only after more social discussions and experience in various use cases of blockchain technology has accumulated to a significant extent.

REFERENCES

[1] Nakamoto S. "Bitcoin: a peer-to-peer electronic cash system," pp 1-9, 2008.

[2] J-H Huh and K. Seo, "Blockchain-based mobile fingerprint verification and automatic log-in platform for future computing," The Journal of Supercomputing, Springer, pp.1-17, 2018.

[3] S-K Kim and J-H Huh, "A Study on the Improvement of Smart Grid Security Performance and Blockchain Smart Grid Perspective," Energies, MDPI, Vol.11, No.7, pp.1-22, 2018.

[4] Yan Chen, "Blockchain tokens and the potential democratization of entrepreneurship and innovation," SSRN, pp.12-13, 2017.

[5] Y Nir Kshetri, "Blockchain's roles in meeting key supply chain management objectives," International Journal of Information Management, Elsevier, 80-82., 2018.

[6] Alexander Savelyev, "Copyright in the Blockchain era: Promises and challenges," Computer Law & Security Review, Elsevier, 2018.

[7] J-H Huh, S Otgonchimeg, and K Seo,; "Advanced metering infrastructure design and test bed experiment using intelligent agents: focusing on the PLC network base technology for Smart Grid system," The Journal of Supercomputing, Springer, Vol.72, No.5, pp 1862-1877, 2016.

[8] Nir Kshetri, "Blockchain's roles in strengthening cybersecurity and protecting privacy," Telecommunications Policy, pp 20-23, 2017.

[9] S-K Kim, U-M Kim, J-H Huh, "A Study on Improvement of Blockchain Application to Overcome Vulnerability of IoT Multiplatform Security," Energies, MDPI, Vol.12, No.3, pp.1-29, 2019.

[10] J-H Huh and K Seo. "Hybrid advanced metering infrastructure design for micro grid using the game theory model," International Journal of Software Engineering and Its Applications, Vol. 9, No. 9, 257-268, 2015.

[11] Richard B. Levin, Peter Waltz, and Holly LaCount, "Betting Blockchain Will Change Everything – SEC and CFTC Regulation of Blockchain Technology, Handbook of Blockchain," Digital Finance, and Inclusion, Elsevier, Vol. 2, 187-212, 2017.

[12] J-H Huh, "Smart grid test bed using OPNET and power line communication," IGI Global, USA, 1-425, 2017.

[13] Christoph Prybila, Stefan Schulte, Christoph Hochreiner, and Ingo Webe, "Runtime verification for business processes utilizing the Bitcoin Blockchain," Future Generation Computer Systems, Elsevier, 2017.

[14] Janusz J. Sikorski, Joy Haughton, and Markus Kraft, "Blockchain technology in the chemical industry: Machine-to-machine electricity market," Applied Energy, Elsevier, 234-246, 2017.

[15] J. H. Huh, "PLC-based design of monitoring system for ICT-integrated vertical fish farm," Human-centric Computing and Information Sciences, 7(1), pp. 1-21, 2017.

[26] J. Park et al., Design of the real-time mobile push system for implementation of the shipboard smart working. In Advances in Computer Science and Ubiquitous Computing, Springer, 541-548, 2015.

[17] J.H Huh, T Koh, and K. Seo. "NMEA2000 ship area network design and test bed experiment using power line communication with the 3-phase 3-line delta connection method," International Journal of Applied Engineering Research, Research India Publications, 10(11), 27789-27797, 2015.

[18] Sullivan, C., Burger, E. (2017). E-residency and blockchain. computer law & security review, Elsevier, 33(4), 470-481.

[19] J-H Huh and K. Seo, "RUDP design and implementation using OPNET simulation," Computer science and its applications. Springer, 913-919, 2015.

[20] Herian R. "Regulating disruption: Blockchain, Gdpr, and questions of data sovereignty," Journal of Internet Law, 22(2), 1, 2018.

[21] Berberich, Matthias, and Malgorzata Steiner. "Blockchain Technology and the GDPR-How to Reconcile Privacy and Distributed Ledgers." Eur. Data Prot. L. Rev. 2- 422, 2016.

[22] J.H. Huh, T. Koh, and K. Seo, "Design of a shipboard outside communication network and the test bed using PLC: for the Workers' safety management during ship-building process," In Proceedings of the 10th International Conference on Ubiquitous Information

Management and Communication, pp. 1-6. ACM, 2016.
[23] Fabiano N., “The Internet of Things ecosystem: The blockchain and privacy issues,” The challenge for a global privacy standard. In 2017 International Conference on Internet of Things for the Global Community (IoTGC) (pp. 1-7). IEEE, 2017.
[24] J-H Huh and K Seo, “Design and Implementation of the Basic Technology for Solitary Senior Citizen’s Lonely Death Monitoring System using PLC,” KMMS, Vol. 18, No. 6, 742-752, 2015.
[25] Andoni M., et al., “Blockchain technology in the energy sector: A systematic review of challenges and opportunities,” Renewable and Sustainable Energy Reviews, Elsevier, 100, 143-174, 2019.
[26] B-G Kim and K Goswami, “Basic prediction techniques in modern video coding standards,” Springer, 2016.
[27] Schwerin S., “Blockchain and privacy protection in the case of the european general data protection regulation (GDPR): a delphi study,” The Journal of the British Blockchain Association, 1(1), 3554, 2018.

Author

Seong-Kyu (Steve) Kim has born in Seoul, Republic of Korea. In Feb. 2006, he graduated from Sungkyunkwan University at Seoul, Department of Information Communication Engineering in Korea and received his master degree. In Aug, 2019, He graduated (Ph.D) from Sungkyunkwan University at Suwon, Department of Electronic and Electrical Computer Engineering. He started his career as a ICT in 1999, and he was before worked Hyundai Information Technology,

He has worked on Hyundai Motor IT R & D Research, Hyundai Construction IT R & D Research, Korea Railroad IT Project, Korea Highway Corporation IT Project, and Ministry of Public Administration and Security IT Project.

He worked at Samsung during 1999 ~ 2017. He was responsible for Saudi Aramco security (physical and information protection) projects, Kuwait KNPC security (physical and information protection) projects, and Singapore Changi Airport security (physical and information protection) projects.

He also lectured on "Introduction to Public Computers" at Songdam University, Yongin. (2010 ~ 2011). Lectured "Security System" at Sungkyunkwan University Graduate School of Information and Communication (2015)

CISA, PMP, CISSP, and CPPG lectures were conducted at Wise Road, an accredited Ministry of Employment and Labor (2010-2016). Computer Engineering Lecture at the Hackers Lab, an accredited Ministry of Employment and Labor (2016)
Lectured on industrial security management at "Olwin Edu" educational institution certified by Ministry of Employment and Labor (2010 ~ 2016). In addition, he received the Best Paper Award at the Korea Multimedia Society (MITA) in 2019.

He has international certifications such as CISA(Certified Information Systems Auditor), CISSP(Certified Information Systems Security Professional), PMP(Project Management Professiona), ITIL Foundation, CCNP, SCJP, ISE, CPPG, ISO 27001, ISO 20000, ISO 9000, ISO 22301 has etc.

Currently he is CEO of "Geoblue Lab" Republic of Korea and “GOB Universal PTE,. LTD” in Singapore. His research interests are Blockchain, AI, Big Data, Smart Grid, Network Security, IoT, App, System Architecture