Mini Review

BIOMEDICAL Journal of Scientific & Technical Research

ISSN: 2574 -1241

DOI: 10.26717/BJSTR.2024.56.008927

Legal Considerations on Personal Information Protection Systems that Use Blockchain

Kouya Takara*

Institute of Library, Information and Media Science, University of Tsukuba

***Corresponding author:** Kouya Takara, Institute of Library, Information and Media Science, University of Tsukuba

ARTICLE INFO

Received: May 31, 2024

Published: June 07, 2024

Citation: Kouya Takara. Legal Considerations on Personal Information Protection Systems that Use Blockchain. Biomed J Sci & Tech Res 56(5)-2024. BJSTR. MS.ID.008927.

ABSTRACT

The purpose of this paper is to present a view on the implementation of blockchain technology that is compatible with Japan's personal information protection legislation. While blockchain is a mechanism that can guarantee the authenticity of information due to its non-falsifiability, it also has privacy risks, such as the persistent storage of privacy-related information, which makes it difficult to correct or delete. This paper introduces examples of blockchain implementations and analyzes the issues that may arise in actual implementations and operations under the Personal Information Protection Act from a legal and interpretive perspective.

Keywords: Japanese Law; Personal Information; Blockchain; Privacy by Design; Act on the Protection of Personal Information

Introduction

The balance between protection and use of personal information has become more important in recent years, as seen in the use of Big Data in Artificial Intelligence (AI) development and the ecosystem for data use by governments in smart and super city concepts. Over 30 years have passed since Dr. Ann Cavoukian, the former Information and Privacy Commissioner of Ontario, Canada, advocated the concept of privacy-by-design in 1995, but the idea that service providers should protect user privacy at every stage from design to use, and so on, has become a global standard today [1]. Of course, although private businesses and government services incorporate system design for personal information protection in their terms of use, regulations, and privacy policies, many cases of personal information leakage are caused by human error; therefore, a mechanism to prevent leakage needs to be built, such as by clarifying the transaction history of such information. Privacy protection mechanisms using blockchain technology have attracted attention in recent years. This technology is also expected to be implemented in the sharing of medical records and prescriptions among medical institutions. Blockchain is the technology underlying cryptocurrencies such as Bitcoin, and has also become that underlying smart contracts to automate contracts in financial transactions.

Some local governments in Japan have recently conducted demonstration experiments on providing administrative services using blockchain technology and are making efforts to implement them. This study contributes to the proper activation of the use of personal information in the future by presenting specific cases of privacy protection systems using blockchain and conducting legal reviews from the perspective of Japan's Act on the Protection of Personal Information [2].

Blockchain and Privacy Protection Systems

Advantages of Blockchain-based Privacy Protection

According to the definition by the Japan Blockchain Association, blockchain refers in a broad sense to "a technology that achieves high availability and data integrity by using digital signatures and hash pointers to create a data structure where it is easy to detect tampering and storing this data in a large number of nodes distributed on a network" [3]. Decentralized management of information is one of the characteristics of blockchain technology, which has the advantages of (1) high availability, (2) high integrity, and (3) low cost of transactions in the management of information [4].

1. Regarding high availability, unlike centralized information management, where a failure of the management system will result in the system stopping function, blockchain-based information management enables the system to operate even if a part of the network is damaged. In addition to operational benefits, this is also advantageous from the perspective of responding to risks from cyberattacks.

2. Regarding high integrity, impersonation is difficult because each information transaction uses encrypted signatures, and further, since transaction data is stored on a chain with previous blocks, tampering is virtually impossible as data tampering would require the tampering of previous data as well. Since the entire transaction history is recorded, one can monitor data tampering in real-time.

3. IN terms of the low cost of transactions, unlike centralized information management, there is no need for a third party for information management, thereby reducing management costs, as only service providers and users may exchange information. Regarding this point, this may lower the barrier to providing services. At the same time, since the service user is personally and directly involved in the transaction of information, the privacy decisions of the individual involved in the transaction of personal information can be better reflected [5].

Implementation Cases

Implementation of Blockchain in Local Governments in Japan: Several demonstration experiments of blockchain technology have been conducted in recent years in local communities under initiatives such as Smart Cities and Society 5.0, with blockchain technology as one of the core technologies. A survey conducted by the Institute for Tokyo Municipal Research [6] revealed that current cases have the following characteristics:

1. Using blockchain as a proof to third parties,
2. Using blockchain to track and record movement history,
3. Sharing information over a wide scale, and
4. Adding new economic value.

One case is the "Iizuka Blockchain Street Concept" announced in Iizuka, Fukuoka Prefecture in 2019, and as a 2020 experiment focusing on data distribution, a demonstration experiment is being conducted to digitize various certificates such as residence certificates using dummy data, that ensure "proof of issuance origin" instead of the official seal (mayor's seal) and "tamper-resistance" instead of copy-protection paper through a blockchain-based trust service. In this experiment, the hash value of the digital signature is recorded in the form of a blockchain to prevent tampering, and the transaction date and time are clarified by a timestamp to prevent tampering. This demonstration experiment was carried out through an agreement between Iizuka City and four companies in the city. In 2021, Iizuka City announced the "Iizuka City Blockchain Promotion Declaration" at the "Fukuoka Blockchain Forum (hosted by Fukuoka Prefecture)," which aimed for city development using blockchain, with industry-academia-government collaboration in the form of a comprehensive project that includes human resource development [7].

Kaga in Ishikawa Prefecture announced the "Blockchain City Declaration" in 2018, and is promoting a smart city concept using internet and communication technology (ICT), in which it aims to issue the "Kaga e-Resident Card NFT" with the Web3 Wallet Management Function using official individual authentication using Non-Fungible Tokens (NFTs) with My Number Cards and the blockchain under the demonstration experiment for electronic voting that links smartphones and the My Number cards, resulting in a "Kaga e-Resident System" to create the "Kaga e-Resident" who is an electronic resident by 2021. In March 2024, an announcement was made that "Kaga e-Resident Card NFT" would be issued on the "Japan Open Chain," a public chain [8]. Nagasaki in Nagasaki Prefecture has started offering an electronic contracting system using blockchain since 2023. Demonstration experiments for this project were carried out in 2021, and it has been operational since 2023 after verifying its appropriateness under the Construction Business Act and the Electronic Signature Act. Blockchain encryption technology uses IC cards with built-in electronic certificates used for electronic bidding and secret keys (wallets) linked to IDs and passwords, enabling settlement without IC cards, and the necessary documents are organized and shared, and agreement information is recorded on the blockchain, making the contract fully digitalized [9]. In addition, Kumamoto in Kumamoto Prefecture, Saga in Saga Prefecture, Bandai in Fukushima Prefecture, and Yabu in Hyogo Prefecture have also been promoting the use and introduction of blockchain. However, across Japan, knowledge about blockchain is lacking or a shortage of technical personnel, initial introduction costs, and so on exists, so the movement toward introduction is not necessarily active [10].

Estonian Healthcare Blockchain: Estonia is currently one of the most digitized countries, with e-IDs and administrative digitization reaching almost 99%. In Estonia, personal information is linked to a personal ID, attributed to an individual, and stored in an encrypted government database. To prevent data tampering, transaction records, and so on are managed as a blockchain, and timestamping for every second is implemented, thereby making it virtually impossible to tamper with (KSI blockchain). In addition, they have managed data collaboration between public and private sectors by decentralizing data in databases to ensure the confidentiality and robustness of information and to ensure secure data collaboration (x-Road) [11]. The development of timestamping technology for blockchain use in Estonia began around 2007, and a system using this technology was introduced in 2012. An example of information management using blockchain in Estonia is medical blockchain. Medical records are digitized, and medical information such as drug prescription information

can be shared between all medical institutions, facilitating appropriate drug prescription and medical treatment [12]. As previously mentioned, transactions with personal information are timestamped every second, so if another individual accesses the medical information, that transaction can be tracked, thus ensuring the integrity of the data. Each use case in Estonia is a representative model case to advance the digitization of governments in the future.

Consent Acquisition Model: Several proposals have been made recently in the academic field for systems to protect personal information using blockchain [13]. Rivadeneira, et al. propose a model to handle personal information based on blockchain technology that builds on some of the features of a conceptual privacy preservation framework called Pacha (Privacy-Aware Component for a Human-in-the-Loop IoT Approach) [14]. The model proposes the use of authorized blockchains to preserve the integrity of transactions derived from both data sharing and consent actions, and aims to address consent management, transparency, and non-repudiation issues in human-centric internet of things (IoT) systems by eliminating a centralized approach and relying on blockchain technology. Human-centric IoT is a focal issue in the current smart city concept and Society 5.0. IoT devices contain a considerable amount of information with high expectations of privacy protection, such as healthcare and lifestyle information, and the secure and low-cost management of such information as well as the ability to fully reflect the intentions of relevant individuals in the context of such information are critical. Although these models have not yet been implemented, future trends in this area will attract attention.

Review based on the Act on the Protection of Personal Information in Japan

Appropriateness of Blockchain in Personal Information Protection Systems

Blockchains can be categorized as public blockchains, which are decentralized, private blockchains, which are centralized under a single entity, and consortium blockchains, which have more than one controlling entity. Public blockchains, in which anyone can participate as a node, are considered highly secure and transparent because the rules cannot be changed by a specific administrator. However, since they openly disclose transaction data, private and consortium types are superior in transactions that involve highly confidential information. Private- and consortium-type blockchains differ in terms of the high degree of decentralization of management authority and information, and many blockchains related to personal information that local governments are considering for introduction are based on the former. Blockchains can also be classified into permissioned and permissionless according to whether they are approved by administrators, and since the latter require approval from participants whose trustworthiness is unknown to finalize transactions, the former is superior in managing highly confidential information. Furthermore, permissionless blockchains may not meet EU GDPR privacy protection requirements [15]. This work reviews permissioned type blockchain with an administrator for information from the perspective of Japan's Act on the Protection of Personal Information (Personal Information Protection Act).

Analysis based on the Act on the Protection of Personal Information

The Japanese Personal Information Protection Act defines a business handling personal information as a person who uses a database of personal information for business purposes, and establishes various obligations regarding the management, use, and transfer to third parties of the personal information held by the business. The 2015 amendment to the Law on the Protection of Personal Data strengthens the provisions for personal participation and establishes the right to claim as a mechanism to ensure the Identifiable person's right to self-determination with respect to the data held by the company. The right to request disclosure (Article 33), correction (Article 34), and suspension of use (Article 35) of personal information from business handling personal information is stipulated. Also, for government agencies, the right to request disclosure (Article 76), correction (Article 90), suspension of use, deletion, etc. (Article 98) of retained personal information and the procedural provisions for these rights have been established. In addition, since the 2020 Amendment, the rules for participation by the Identifiable person have been further strengthened [16].

It is understood that the human right of individuals protected by the Personal Information Protection Act is the right to privacy, and the Supreme Court has also expressed the view that it is the right not to have personal information disclosed to third parties [17]. In other words, from the perspective of the right to privacy, it is generally understood that personal information should be under the control of the identifiable person unless there is a justifiable reason. The Personal Information Protection Act is a law whose purpose is to protect the appropriate use of personal information while protecting the privacy of individuals [18]. Therefore, businesses are required to handle personal information in an appropriate manner that reflects the intent of the identifiable person, although there are differences in the degree to which the type of personal data (e.g., anonymized processed information, pseudonymized processed information, etc.) is handled. The following is a review of the applicability of the Personal Information Protection Act to the use of blockchain from the perspectives of personal information management and the reflection of the will of individuals.

Management of Personal Information: Businesses handling personal information are required to specify the purpose of use when acquiring personal information (Article 17), notify the identifiable person of the purpose of use (Article 21), acquire the information in an appropriate manner (Article 20), prohibit in principle the handling of personal information outside the scope of the purpose of use without the consent of the person (Article 18), and prohibit inappropriate

use (Article 19), The law also prohibits the improper use of personal information (Article 19) and restricts the provision of personal information to third parties (Article 27), thereby requiring the proper handling of personal information that reflects the will of the individual, from its acquisition to its use. While the data of personal information in one's possession must be authentic (Article 22), if the transaction records of such personal information are block chained, in addition to the approval process at the time the transaction is finalized, the entire transaction record can be referenced retroactively, thus ensuring the data's non-falsification. The retroactivity of transaction records will also contribute to reducing the risk of leakage from the perspective of the obligation of business handling personal information to supervise employees (Article 24) and subcontractors (Article 25) to ensure that personal information is handled appropriately. On the other hand, as for the authenticity of data, the second sentence of Article 22 states that "Efforts shall be made to erase said personal data without delay when there is no longer a need to use it," so if personal information itself is block chained, not only the transaction history but also the data itself can be guaranteed to be non-tampered with. However, this requirement cannot be met because the data cannot be modified or deleted.

In addition, when personal information is managed and transactions are approved in a decentralized manner among multiple businesses, such as in the case of a consortium-type blockchain, the issue of provision of personal information to a third party arises. The Personal Information Protection Act stipulates in Article 27, Paragraph 1, that in principle personal information may be provided to a third party only with the prior consent of the identifiable person to whom the information pertains. However, Article 27, Paragraph 2 of the Act stipulates that personal information may be provided to a third party without the consent of the person in exceptional cases, provided that the 8 requirements, such as the purpose of providing personal information to a third party, are fulfilled in advance. In item 6, "the fact that it will cease to provide personal data that can be used to identify the person to a third party at the request of the A system that makes it difficult to delete personal information itself will not meet this requirement, making it virtually impossible to provide personal data to a third party on an opt-out basis. In addition, when conducting global transactions, there may be a conflict with personal information protection legislation that establishes the right to request and the obligation to delete data, such as the right to be forgotten (right to erasure) under Article 17(1) of the GDPR [19]. Even though the second sentence of Article 22 on personal information is only an effort provision, it is desirable that even a permissioned blockchain with a controller should not contain personal information itself. Similarly, appropriate management of personal information is stipulated for government agencies, etc., and the above issues surrounding blockchain and personal information in business handling personal information may be applicable.

Identifiable Person's Participation: As mentioned above, the Personal Information Protection Act since the 2015 amendment stipulates the right of the individual to make various types of requests, and the influence of the Identifiable person in the way and the eligibility of the content of personal information held by business handling personal information and government agencies, etc. has become stronger. As already mentioned in (i) above, if personal information itself is recorded on the block, it becomes virtually impossible to correct or delete such personal information when the need for correction or deletion arises at the request of the Identifiable person. Identifiable information would therefore leave the control of the person, and the request for privacy protection would not be fully satisfied. Therefore, as mentioned above, it is appropriate for a privacy protection system using blockchain to function as a ledger to record transaction history. In addition, when an opt-out method is used in the provision of personal information to a third party, Article 27(2)(v) stipulates the requirement that "the means or manner in which it will provide the data to the third party" be clearly indicated to the Identifiable person. This is because the means of provision is considered to be closely related to the damage to the Identifiable person resulting from the transfer of information. The method of provision will be indicated here, such as whether the information will be provided online or whether it will involve the transfer of physical media, such as by mail. If the privacy protection system using the blockchain is used as a ledger of transaction history, it can be said that it does not fall under the method of provision itself. If the personal information itself is recorded on the block, then this system would be a method of provision to a third party, but as mentioned earlier, this method is difficult to adopt for an opt-out method because it is difficult to correct or delete the information.

Conclusion

I discussed blockchain-based personal information protection systems. This is an analysis from a legal perspective only, and the technical aspects of blockchain are based on previous studies. In the context of privacy protection, personal information protection systems using blockchain technology may reduce the risk of falsification or leakage of personal information from the perspective of transaction transparency and data integrity of such information, and contribute to the protection of data privacy rights by reflecting the will of the service user. On the other hand, blockchainization of personal information itself entails privacy risks due to the difficulty of tampering with that information. Therefore, it would be appropriate in the current situation to introduce it as a system to guarantee the security of information transactions, combined with cloud storage and other information storage technologies. From the perspective of privacy-by-design, research and development are expected to continue, but in the future, I would like to continue to analyze and study cases in Japan where such systems have been introduced.

Acknowledgements

This work was supported by JSPS KAKENHI Grant Number 20K13385. I would like to thank Editage (HYPERLINK «http://www.editage.com»www.editage.com) for English language editing.

References

1. Ann Cavoukian (2009) Privacy by Design: The 7 Foundational Principles. Office of the Information and Privacy Commissioner of Ontario. Retrieved March 18, 2018. See Masao Horibe and JIPDEC (Edi.) (2012). Privacy by Design. Nikkei BP.
2. In interpreting the Personal Information Protection Act, reference is made to the following. Primavera De Filippi and Aaron Wright (2018) Blockchain and the Law: The Rule of Code. Translated by Naoto Katagiri (Edi.), et al. (2020). Kobundo; Katsuya Uga (2021) Explanation of the new Personal Information Protection Act, article by article. Shin Kojin-Joho Hogo Ho no Chikujo Kaisetsu. Yuhikaku; Itsuo Sonobe and Shizuo Hujiwara(Edn.) (2022) Explanation of Personal Information Protection Act (Kojin-Joho Hogo Ho no Kaisetsu) (3rd Edn.)., " Gyosei; Personal Information Protection Commission Japan; Ministry of Justice: Japanese Law Translation.
3. Japan Blockchain Association (2016) Definition of Blockchain" is now available.
4. (2018) Ministry of Internal Affairs and Communications, Japan (2018) Information and Communication in Japan: White Paper 2018, p. 35.
5. Jorge Eduardo Rivadeneira, María B. Jiménez,Radu Marculescu, André Rodrigues, Fernando Boavida, et al. (2023) A Blockchain-Based Privacy-Preserving Model for Consent and Transparency in Human-Centered Internet of Things. IoTDI '23, etc.
6. (2022) The Institute for Tokyo Municipal Research. Research and Study on the Use of Blockchain Technology in Basic Municipalities.
7. (2022) Iduka city. A proof business outcome for practical use of the administrative documentary electronic issue for which block chain technology was utilized is exhibited.
8. See Kaga E-Residency.
9. Toshiba (2023) Launched a blockchain-based electronic contracting system.
10. (2022) See The Institute for Tokyo Municipal Research.
11. (2023) See e-Estnia. Estonian Blockchain Techinology.
12. See e-Estonia. "e-Health".
13. See Rivadeneira, et al. (2023), pp. 302.
14. Rivadeneira, et al. (2023), pp. 303.
15. (2018) EU Blockchain Observatory and Forum. "Blockchain and the GDPR".
16. Prior to the revision of the Personal Information Protection Act, the right to request suspension of use, erasure, etc. was limited to cases of violation of the Act, such as cases of use for other than the intended purpose or provision to a third party. With the amendment, the right to request cessation of use, erasure, etc. is also recognized in cases where there is no longer a need to use personal information, in cases of serious leakage that must be reported to the Personal Information Protection Commission, or in cases where the rights or legitimate rights of the Identifiable person may be harmed.
17. Supreme Court of Japan, December 24, 1965 (Keishu, vol. 23, no. 12, p. 1625); Supreme Court of Japan, March 6, 2008 (Minshu, vol. 62, no. 3, p. 665), etc.
18. Personal Information Protection Act, Article 1.
19. In addition, under the 2020 amendment to the Personal Information Protection Act, the Japanese Personal Information Protection Act will be applied extraterritorially (Article 171) when handling the personal information of Japanese residents and others.

ISSN: 2574-1241

DOI: 10.26717/BJSTR.2024.56.008927

Kouya Takara. Biomed J Sci & Tech Res

Submission Link: https://biomedres.us/submit-manuscript.php