Self-Sovereign Identity and Blockchain-Based Content Management

Yusuke Kurihara

Self-Sovereign Identity and Blockchain-Based Content Management

Yusuke Kurihara [1-2][0000-0001-6590-3495]

[1] Graduate School of Media and Governance, Keio University, Kanagawa, Japan
[2] InfoCom Research, Inc, Tokyo, Japan
yukurihara.cyberlaw@gmail.com

Abstract. The concept that a person aims to control my own identity without the intervention of a controlling entity is called self-sovereign identity (SSI). The SSI is an antithesis to the phenomenon that certain companies and organizations, called digital platformers, collect data centrally.
This paper expands the concept of SSI and describes the possibilities and problems when applying it to self-content management using the concept of Self-Content Management (SCM). In particular, I discuss the possibility of self-sovereign management of digital content, and discuss DRM using blockchain technology as a means.
This paper is assumed that SSI can be applied to content created by myself, but by properly managing content using blockchain technology, it is possible to complete licenses and levy fees. I also clarified that it could be a substitute for the resale right.
As a result, SCM promoted the problem of "orphans' works" and facilitated the processing of rights, and revealed that it could contribute to the further development of culture. However, I also address that there are two issues. One is the lack of institutional trust, rather than the technical credibility of the blockchain. The second is consistency with the Attorney law of Japan.

Keywords: Self-Sovereign Identity (SSI), Self-Content Management (SCM), The Blockchain-based Digital Right Management (DRM).

1 Introduction

1.1 Personal Data, Know Your Customer and Self-Sovereign Identity

When you buy cigarettes or alcohol at a convenience store, a clerk asks you to press an adult confirmation button in Japan's regulations. When purchasing online, you enter your password, personal account info, and address and credit card number to receive a delivery at home. This is just one example of various daily services that require the presentation of an individual's identity in a verification called Know Your Customer. This information, including purchase history, is then collected by a company, regardless of whether customers are conscious or not, and analyzed and used for direct advertising.

In the digital society, the management of digital identities is becoming increasingly important as sensitive information regarding things like financial accounts and medical care is digitized. The “information bank” has become a hot topic in Japan.[1] The concept of “controllability” is based on the concept of companies and organizations becoming central management organizations to collect and utilize data. Consumers receive a reward equivalent to the provided personal data (which is sometimes used for the public interest).

However, what central management organizations collect individual digital identity is risk because digital security is a concern, and even trusted international companies have experienced large-scale leaks. Regulating agencies have become more involved in investigating and applying sanctions to companies involved in data breaches. In particular, general data protection regulation (GDPR), which came into force in Japan in May 2018, is prominent. The maximum fine imposed for a violation of the GDPR is (1) €1,000 million or 2% of total sales for the previous fiscal year, whichever is higher; or (2) €2,000 million or 4% of total sales. Since its implementation, the GDPR has led to significant fines, as published by national data protection agencies.[1]

While there is no comprehensive data protection law in the United States, Chinese video application TikTok settled with the U.S. Federal Trade Commission in 2019 through a $5.7 million fine for allegedly obtaining personal data of children without parental consent in violation of COPPA (The Children's Online Privacy Protection Act).[2]

In recent years, data protection legislation has grown in popularity. CCPA (The California Consumer Privacy Act) has been in force since January 2020. African countries such as South Africa and Egypt have enacted data protection laws similar to the GDPR, while Association of Southeast Asian Nations countries such as Singapore and Indonesia have also enacted new data protection laws in recent years. In Thailand, data protection legislation similar to the GDPR has been introduced in Parliament. In China and the Philippines, data localization, which mandates the domestic preservation of personal information and important infrastructure data, is stipulated. This proves the importance of the data and the regulation against the threat of data concentration in the enterprise.

Alternately, there is the concept of self-sovereign identity (SSI). This concept is intended to allow individuals to control their own identity without the intervention of a management body.[3] As an antithesis to the centralization of data in businesses and governments, it is attracting attention as one of the ideal forms of digital identity.

---

[1] An information bank reliable entity to which a person delegates the provision of personal information to a third party to the extent that the person agrees, with the aim of promoting the distribution and use of personal data by enhancing effective personal involvement (controllability) (Ministry of Economy, Trade and Industry Study Group on Approaches to Certification Schemes for Information Trust Functions "Guideline on Authorization of Information Trust Functions ver. 2.0 [October 2019]").

1.2 Non-Personal Data/SSI/Self-Content Management

In Europe, a distinction is made between personal and non-personal data, such as industrial information. In Europe, the GDPR states that the protection of personal, but not non-personal, data is a fundamental right. However, to ensure the free flow of information, the "Framework for Free Distribution of Non-Personal Data in the EU (REGULATION (EU) 2018/1807 OF EUROPEAN PARLIAMENT AND OF THE COUNCIL of 14 November 2018 on a framework for the free flow of non-personal data in the European Union)" prohibits requiring the storage and processing of data within the territory of a specific country or preventing the storage and processing of data within other countries.

The collection of industrial data also assumes that the distribution of information is an essential aspect of corporate globalization. However, if the concept of SSI is applied to non-personal data, the individual should be able to control whether the data is distributed freely. It should be up to the individual to decide whether to distribute his or her non-personal data abroad even when the company's servers are abroad.

One example of this issue is music ownership. In Japan, most music copyrights have been transferred to JASRAC in trust, and JASRAC has centralized management. It has eased facilitation of the rights management between music users and numerous composers and songwriters and has also aided in making appropriate allocations. But outside of music, things aren't going well. Content created by a professional is a manifestation of his or her own personality, and his or her own work should constitute non-personal data, based on the SSI philosophy, so that he or she can have appropriate control and involvement over the data.

In recent years, blockchain technology has been replacing centralized content management.[4] Content management is also getting attention from the content market.[5] According to the network externality of the platform service, the blockchain's copyright management system may lead to a paradigm shift in the centralized copyright management model and content delivery methods of JASRAC[6] using the digital rights management (DRM) 2.0 that SSIs bring.[7]

In this paper, therefore, we examine the prospects and challenges of content creators using blockchain technology to appropriately implement SCM (Self-Content Management) based on SSI.

2 Self-Sovereign Identity (SSI)

2.1 Concept of SSI as Ideal Models for Secure Data Protection

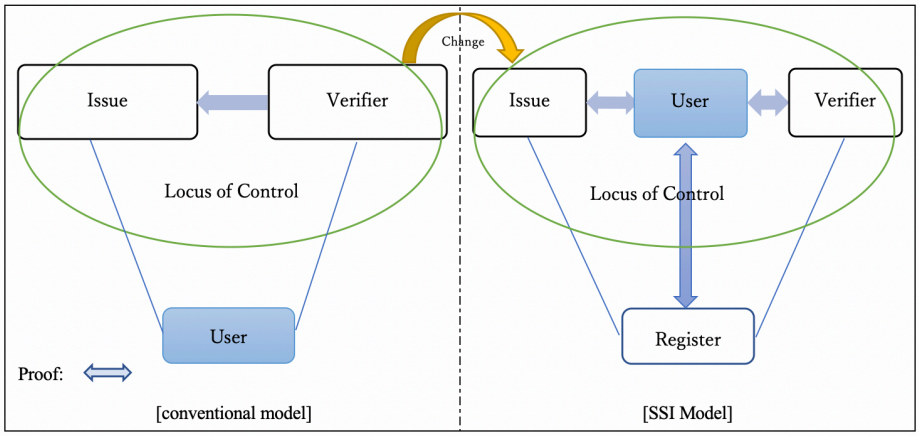
In short, self-governing identity means that one's own identity is one's own management. Most service providers, including the four[8] biggest providers—Google, Apple, Facebook, and Amazon—collect and use some personal data, and they maintain and manage this data centrally. Naturally, this data use is optional. Google's privacy policy, for example, states that "You can adjust your privacy settings to control what we collect and how your information is used." Thus, "controllability" is left to the user. Also, in the Google Terms of Service, there is in the item of "Modifying and Terminating our

Service" that reads, "We believe that you own your data and preserving your access to such data is important." The idea of digital identity is an antithesis to the centralization and use of data by companies.

With regard to data, in Japan it is used "ownership" not "Syoyu-ken" which means same definition of ownership in Japanese. However, it is well known that ownership of data cannot be conceived. Also, if there's really "ownership" in the data and it's accessible, then there's no need for Google to get involved, nor is there a need for such a sentence. This statement shows that there are principles and practices.

Christopher Allen, a leading proponent of SSI, suggests that "A vision of how we can build trust in our digital identities while maintaining individual privacy" is SSI.[9]

Fig. 1. Changes in the model for KYC (From conventional to SSI) [10]



As shown in Figure 1, the user is at the center of SSI. In the conventional model, the user is not involved in managing his or her own identity, and authentication can only occur between the issuer and the authenticator. In the SSI model, the user is actively involved in managing his or her own identity, plays a central role, and without user authentication, no personal data is transferred between the issuer and the authenticator.

The concept of SSI is based on the fact that personal data are subject to governance without external factors. The following six characteristics are listed:[11]

1. Complete control of the data
2. Ensuring the security and privacy of users' personal data
3. Full data portability
4. No need for trust in central institutions
5. Ensuring data integration
6. Maintaining transparency of personal data

This concept also attracts attention because it is expected that the incidents will be reduced because companies are not centrally storing data.[12]

2.2 Social Implementation Level

The SSI model is gaining attention because it provides a solution to data protection legislation such as the GDPR rather than merely providing a strong sense of empathy and support for ideas. Blockchain technology is attracting attention as a platform for social implementation of these solutions. Blockchain technology is a peer-to-peer (P2P)-based consensus-building system that does not require a central authority and does not apply only to cryptographic assets. P2P-based blockchain technology acts as a trusted third-party replacement because, in the SSI model, blockchain technology satisfies the six elements described in Section 2.1.[2]

In Europe, the European Commission established the European Union Blockchain Observatory and Form in February 2018. In May 2019, a theme report entitled "Blockchain and Digital Identity" was issued.[13] It emphasizes a blockchain technology-based concept centered on personal data with autonomous and distributed identities in the EU. In Europe, personal data are defined as "right to be forgotten" and data access rights and automatic processing provisions in the GDPR as the right to ensure a person's identity.[3] In the case of blockchains, there are aspects that are difficult to implement, especially in relation to the right to correct or forget. In other words, the technical feature that it cannot be modified after the fact is a means of ensuring credibility. Therefore, in principle, it cannot be addressed in relation to the right to correct or to be forgotten.[4] It also includes the smart contract,[14] which eliminates the possibility of external factors intervening in the realization of an electronic protocol for handling the terms and conditions of a contract, and blockchain is applicable.[15] Therefore, the SSI model is based on blockchain technology.

Blockchains are not centralized, but they are P2P based and are sometimes referred to as “Decentralized Identity (DID)”. In the same way as SSI, the user keeps his or her own personal data but cooperates within the range permitted by the user.

---

[2] Abraham[11] at 7

[3] European Union Blockchain Observatory and Form [13] at 19

[4] Turning away from this discussion, the GDPR response in the blockchain, in particular the right to correct and the right to be forgotten, can be cleared by:.

In the real estate registration records of Japan, correction before and after correction, such as ex officio correction, is distinguished by an underline, so this should be followed. In other words, before and after the correction are clearly indicated. Since it is practically impossible to directly rewrite the original data before correction on a blockchain basis, the corrected information is written by specifying the corrected part.

Next, in relation to the right to be forgotten, it is necessary to ensure that no corrections are left even in the right to correct mentioned above. For the time being, this response could be addressed by not granting any access privileges on a blockchain-based basis. However, if it is not observable ex post facto, the reliability cannot be maintained, so it is necessary to separate the data groups that exercised the right to be forgotten. In this way, it is possible to solve the problem. However, it is necessary to examine whether leaving traces of the exercise of the right to be forgotten is sufficient guarantee of the right to be forgotten.

2.3 ERC 725/ERC 735

In fact, the concept of DID is indispensable for the social implementation of SSI. Section 2.3 describes several use cases (See, Table 1). In one of the use cases, Ethereum developer Fabian Vogelsteller presented a draft SSI standard on GitHub called Ethereum Request for (ERC) 725.[16] ERC 735 is the relevant standard for adding and deleting claims of ID Smart Contracts in ERC 725.

ERC 725 can be defined to assign IDs not only to people but also to organizations, devices, software, etc. and can be considered one of the social implementations of SSI. In addition, ERC 725 allows the transfer of assets and rights as well as personal data.

1. ERC 725–v2: Proxy Account Standards [17]
2. ERC 734: Key Management Standards [18]
3. ERC 735: Claim Holder Standard [19]

Table 1. The use case of ERC 725/735[20]

Project Name	Use Case Description
Origin	ERC 725 is used as the basis for Origin's user ID. ERC 725 was selected for interoperability optimization. Origin users have a public profile that includes proof of email, phone number, social networking service account, etc.
Caelum Labs	ERC 725 will be used as a basic local and national identity system for Ethereum-based blockchains. The main goal is to use it to establish trust between people, companies, and governments, so smart contracts can be used in any process between them.
Hydro	Hydro plans to provide a platform layer to facilitate and improve aspects of the dApp development process, including identity management. Accordingly, Hydro plans to offer developers a standard implementation of ERC 725 in conjunction with other identity standards that can meet the specific needs of its applications. These identity standards are detailed in the ERC 1484 reference repo.
LydianID	Lydian Ventures is using ERC 725/735 identities and investigations on several projects and created LydianID as an identity management dApp. LydianID is currently being used by academic institutions to certify on blockchain the studies of their students, who can share the attestation with others. ERC 725/735 identities are used in other projects where interoperability among several parties is required and a role-permission system is built with investigations.

Project Name	Use Case Description
Smilo	Smilo is using ERC 725 identities and off-chain claims including Facial Biometrics. Our first implementation contains festival/opera/station facial authentication based on a DID + ticket number. We want to collaborate on a global standard to make interoperability work, and PII is shared in a secure way.

2.4 Degree and Course Registration Certificate

Globally, blockchain technology is being applied to school records, such as degree certificates, used to fake academic credentials. In Japan, a survey report on the applicability of blockchain technology in universities and research institutions was compiled in April 2019 on the themes of degrees, academic records, and research data.[20] In December 2019, Muroran Institute of Technology and NTT West announced a joint research and development program in order to promote efforts to solve problems in the development of recurrent education in the future.[21]

According to this NTT West's press release[22], that shows compliance with the GDPR and other regulations. However, the necessity of complying with the GDPR is not necessarily high in the case of educational attestation certificates in Japan. However, there is a possibility that issuers will disappear due to consolidation. It is an effective means to avoid such risks and to enhance credibility. It is also advantageous for school management in terms of management costs.

3 How does SSI fit into DRM?

3.1 DRM and Blockchain Technology

Blockchain DRM for non-personal data mainly refers to copyright management, but contents may also include music and photos. Experimental blockchain-based DRM has existed since 2015. In February 2019, JASRAC said it would introduce blockchain into its music royalty management system. Table 2 lists several current instances of blockchain DRM use around the world.

Table 2. The use case of DRM with blockchain-based systems

Name	Summary
Ascribe (Germany)	Art work management service. Artists can easily register their work and manage ownership transfers, loans, and

	sales history with a work certificate issued by the company, which provides a means to deliver a work that meets the artist's needs.
Bound (Americas)	Blockchain image rights management platform. If an image is registered in a procedure similar to a social media posting, a unique certificate is issued, and a legitimate right can be claimed through the certificate.
KodakOne (Japan)	Blockchain image rights management platform. It automatically monitors websites for unlicensed use of registered images and, if found, executes licensing (smart contract). It also automates the purchase of photos and can prove photo rights.
Startbahn (Japan)	Blockchain artwork management system. This service records, manages and shares the history of works of art using the blockchain, tracking who buys art and returning a portion of the transaction value to the artist for each resale.

3.2 SCM: Potential SSI for Content

There is a view that “creation”, which is one of the requirements for works under the Copyright Act of Japan, is an expression of individuality. The expression of individuality means that a work has one identity, or a similar nature, representing the individual. That is why the moral rights of authors include the right to publish, indicate one's name, and maintain integrity. If the content is distributed, the right to publish is likely to be waived, but the right not to request the name of the author and not to alter the content should be protected even for digital content.

In addition, the copyright holder must be guaranteed the rights of reproduction, public transmission, and adaptation, which are among the subsidiary rights of copyright, because reproduction and modification are easy in a digital environment.

Therefore, in order to realize SCM, it is desirable to include direct contract at the outset. The centralized management system of JASRAC comes from the complexity of rights processing. The smart contract allows the company to handle a larger number of theoretical direct contracts, and the technology that supports it is positioned as a blockchain.

SCM is positioned as a means of realizing SSI's philosophy in the content field. This SCM is the realization of the fixation of subjects and objects in information goods. Koichiro Hayashi once advocated a “digital creation rights” as a copyright system for the digital age, as digitization has made it easier to reproduce content.[24] In addition, in terms of the rights to personal data, a comparison of the ownership approach and the copyright approach has been made from the perspective of the subject and object of information.[25]

In conclusion, Hayashi claims the following; The developing digital environment has created this series of trends as consumers become aware that information goods can be

freely and easily reproduced, that it becomes difficult to identify an object by the circulation, and by the circulation, the subject of the information goods becomes unclear. Criticizing the centralization of traditional DRM, Lessig worried about the coming of a controlled society. Lessig's concept of commons is set as an antithesis to the managed society.

The theories proposed by Hayashi and Lessig were tools for the purpose of balancing the return of copyright privileges to creators with free content usage. The SCM fulfills these objectives. In effect, the purpose is realized by the architecture based on the current system.

In other words, according to Hayashi's theory, SCM based on SSI aims to achieve complete control on the premise that the creator takes the initiative and owns the content he or she creates. This control means that the licensing process, including the collection of license fees, is completely self-contained without the intervention of an agent. There is no need for a centralized governing body such as JASRAC, and because it is based on SSI, it is not "administered," as Lessig criticizes.

The SCM is also about blockchain-based, leak-free rights management or just compensation. In the past, in France, the patron system collapsed and painters could not make a living, so the resale right was born; the architecture of the blockchain mirrors the resale right. (At present, the resale right is not permitted in Japan, although there is an opinion for guaranteeing the legitimate interests of the artist that it should be introduced.) The SCM also provides an alternative to the resale right.

In addition, Chang points to the possibility of direct blockchain-based management.[5] However, she claims the blockchain-based DRM can solve the technical issue but it remains the problem of the commercial practice. She points out that this could help eliminate Orphan Works. From a broad perspective, solving this problem will also help eliminate the difficulty of rights processing in digital archiving of cultural resources.

4 Conclusion

The GDPR focuses on the sovereignty of data subjects. I explained that the corresponding blockchain technology, as well as efforts and use cases to implement it, is being discussed in the EU. DRM is this application. Until now, however, it has been difficult for creators to keep their data and manage the rights to the content they create due to the many legal and technical challenges. The concept of SSI applies to both personal data and content, which have become commonplace utilizations.

However, the following two points remain to be addressed. First, blockchain-based rights management is concerned with the "trust" of certificates issued at the time of registration. This trust is not sufficient if blockchain systems cleared the technical standard. In the absence of social recognition, there are no proof documents to use in court. Therefore, the remaining challenge to achieve SSI is not the establishment of laws but the creation of a "trust." If this trust comes from government certification, it could be back to the centralized systems for gathering personal data and content.

[5] Yeyoung[26] at 255

Whether managed by a third party or by industry guidelines, best practices will be an issue for the future.

Second, there are several legal issues. Problems remain with Legal Tech (the information technology to assist the legal affairs)'s relationship with Section 72 of the Attorney Act of Japan and Section 109 the Attorney Act of Korea(provisions prohibiting, as a business, the provision of legal services, etc. for the purpose of receiving remuneration in relation to another person's legal case).[27] Lately, in the Cologne district court in Germany, legal tech was found to be in violation of the legal services act (Rechtsdienstleistungsgesetz), which has similar provisions (LG Köln, Urt, v. 8.1.2019 - 33 O 35/19).

The concept of DID addresses the right to "own," so there are few problems with strangeness. However, in a consortium-style SCM based on the SSI concept, strangeness becomes a problem with the enforcement of other members. Furthermore, enforcement and rights disposition are problematic in relation to the nature of the case. For details, see Matsuo's thesis.[27] However, the paper concludes that there are separate considerations for services, and this is also a future issue.

Despite the problems described above, the concept of SCM is important in preserving creative works for future generations. In the digital archive of cultural resources, the problem in the rights-handling process is orphan works. Because of increasing numbers of orphan copyrighted work and more unusable content, it is a tragedy for copyright holders and authors that the lack of a copyright holder leads to a decline in culture. It is necessary to recognize that rights management by SCM leads to "cultural development" (Article 1 of the Copyright Law of Japan). We hope that this paper will contribute to the development of a society in which individuals have an identity for content and respect it, just as SSIs do.

Acknowledgments. The author wishes to acknowledge Dr. Kunifumi Saito, Associate professor of Law Faculty of Policy Management, Keio University, for his help in interpreting the significance of the results of this study.

5 References

1. Kurihara, Y.: Regulatory enforcement cases and analysis after one year of implementation of the GDPR. InfoCom T & S World Trend Report 365, 29-33 (2019)
2. FTC Website: Video Social Networking App Musical.ly Agreements to Settle FTC Allegations That it Violated Children's Privacy Law. https://www.ftc.gov/news-events/press-releases/2019/02/video-social-networking-app-musically-agrees-settle-ftc, last accessed 2020/08/21.
3. Nomura Research Institute: Digital Identity: Autonomous and Distributed Identity. https://www.nri.com/-/media/Corporate/jp/Files/PDF/service/ips/technology_1.pdf?la=ja-JP&hash=255BF197AD405C48800CED1B7FFFDD98A93A5CDE, last accessed 2020/08/21. NRI Secure Technologies, Ltd., JCB (2020)
4. Nakamoto, S.: Bitcoin: A Peer-to-Peer Electronic Cash System. https://bitcoin.org/bitcoin.pdf, last accessed 2020/08/21. (2008)

5. Kishigami, J.: The Blockchain-based Digital Content Distribution System. Future Generation Computer Systems 89, 746-764 (2018)
6. Savelyev, A.: Copyright in the blockchain era: Promises and challenges. Computer Law & Security Review 34(3), 550-561 (2018)
7. Finck, M. le & Moscon, V.: Copyright Law on Blockchains: Between New Forms of Rights Administration and Digital Rights Management 2.0. IIC-International Review of Intellectual Property and Competition Law 50, 77-108 (2019)
8. Galloway, S.: The Four: The Hidden DNA of Amazon, Apple, Facebook, and Google. Portfolio. (2017)
9. Allen, C.: The Path to Self-Sovereign Identity. April 25, 2016. http://www.lifewithalacrity.com/2016/04/the-path-to-self-soverereign-identity.html, last accessed 2020/08/21.
10. Medium. Self-Sovereign Identity: Shifting the Locus of Control. https://medium.com/@trbouma/self-sovereign-identity-shifting-the-locus-of-control-10da1c8757ad, last accessed 2020/08/21.
11. Abraham, A.: Whitepaper Self-Sovereign Identity, (2017) https://www.egiz.gv.at/files/download/Self-Sovereign-Identity-Whitepaper.pdf, last accessed 2020/08/21.
12. Ogawa, A.: What Is the Self-Sovereign Identity? The New Potential of Blockchain" Info-Com T & S World Trend Report, No. 346 (2018)
13. European Union Blockchain Observatory and Form. Blockchain And Digital Identity, https://www.eublockchainforum.eu/sites/default/files/report_identity_v0.9.4.pdf, last accessed 2020/08/21. (2019)
14. Szabo, N.: The Idea of Smart Contracts. Nick Szabo's Papers and Concise Tutorials, 1997. http://www.fon.hum.uva.nl/rob/Courses/InformationIn-Speech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_idea.html, last accessed 2020/08/21.
15. Hopf, S.: Blockchain Technology Impacting Property Rights and Transaction Costs Regimes, Twenty-fourth Americas Conference on Information Systems, New Orleans, (2018)
16. ERC-725 Ethereum Identity Standard Wecsite. https://erc725alliance.org/, last accessed 2020/08/21.
17. Fabian Vogelsteller frozeman, ERC: Proxy Account #725. https://github.com/ethereum/EIPs/issues/725, last accessed 2020/08/21.
18. Fabian Vogelsteller frozeman, ERC: Key Manager #734. https://github.com/ethereum/EIPs/issues/734, last accessed 2020/08/21.
19. Roelen, E.: https://github.com/ERC725Alliance/erc725/blob/master/docs/use-cases.md
20. METI of Japan, Ministry of Economy, Trade and Industry FY 2018 Industrial Technology Survey Report. https://www.meti.go.jp/press/2019/04/20190423002/20190423001-1.pdf, last accessed 2020/08/21.
21. Nihon Keizai Shimbun (December 2, 2019). https://www.nikkei.com/article/DGXMZO52864490S9A201C1L41000/
22. NTT West Website. https://www.ntt-west.co.jp/news/1912/191202a.html, last accessed 2020/08/21.
23. Kishigami, J.: The Blockchain-based Digital Content Distribution System, 2015 IEEE 15th International Conference on Big Data and Cloud Computing https://ieeexplore.ieee.org/document/7310737, last accessed 2020/08/21.
24. Hayashi, K.: Toward a Soft Copyright System. Copyright Law and Economics, Keiso Shobo. 227-248 (2004)

25. Hayashi, K.: "Relationship between personal information rights and property rights, and between subject and object" Information Security General Science 7, 1-40 (2015)
26. Chang, Y.: Opportunities and challenges of using blockchain technology for copyright registration and contents licensing. Dokkyo Law Review No. 105, 231-256 (2018)
27. Takayuki, M.: Analysis on LegalTech and Attorney Act of Japan" Information Network Law Review. 18, 1-23 (2019)