IPSJ SIG Technical Report
Vol.2019-CLE-27 No.5
2019/3/20

Regular Paper

Decentralized e-Learning Marketplace: Managing Authorship and Tracking Access to Learning Materials Using Blockchain

Patrick Ocheja[1,a)] Brendan Flanagan[2,b)] Hiroaki Ogata[2,c)]

Abstract: The difficulty in protecting and enforcing Intellectual Property (IP) rights has been a major obstacle to sharing intellectual works in digital forms. In this work, we present a prototype design for a decentralized e-learning marketplace where teachers, authorized publishers and authors can publish their learning materials, establish conditions for allowing access, and grant or revoke access based on adherence or infringement of their rights. Using the Blockchain of Learning Logs (BOLL) and a digital book reader (BookRoll), we demonstrate how authors can be empowered to deploy smart contracts that protect and enforce these rights on their intellectual works in a distributed manner. We particularly use the blockchain in order to enable trust, trace-ability, rights protection, transparency and collaboration between authors and users of their work with no third party interference. Finally, we examine the implications of our proposed design, its limitations and directions for future work.

Keywords: intellectual property, copyright, elearning, education, privacy, security, blockchain, smart contract, BOLL, BookRoll

1. Introduction

Digital revolution has continued to redefine how we use and share information including news contents, innovations, educational resources, and contents for entertainment [1]. As the amount of data in the digital space continue to grow leading to more meaningful use cases, it is important to ensure appropriate use, reward ingenuity and foster collaboration among diverse parties. Intellectual Property Rights (IPRs) are rights that allow creators or owners of industrial properties (patents for inventions, trademarks, etc.) or copyrighted works (books, poems, artistic works, etc.) to benefit from their own work or investment in a creation by defining terms of usage which potential users of their work should comply with [3]. With many works on the use of technology to solve issues relating to IPRs protection and enforcement such as [9, 10, 12, 13, 15, 16], we focus on specific issues on how educators including students and teachers can share learning materials in a secure, privacy-enabled, intellectual rights-aware and collaborative environment.

In various e-learning environments, it is common to have teachers share learning resources such as slides, lecture notes, books, quizzes and assignments with their students. Students could in turn also make meaningful use of these resources to arrive at new resources that other students or the teacher might find helpful. With more knowledge resulting from simple interactions like this, we consider it necessary to have a system that supports exchange of these resources, reward ingenuity, increase distribution, foster collaboration, and protect the intellectual rights of the authors. The need to provide answers to the following questions makes this problem worth solving.

1.1 Research questions

(1) How do we ensure trust and transparency between an author of a work that is made available to students and paid for by another organization based on the usage quota of each student without using a third-party? E.g.
   (a) A government can contract a publisher to provide elementary school textbooks on various subjects to all students in digital forms. If the government agrees to pay the publisher based on the number of interactions the students had with the provided textbooks, how can we ensure the existence of verifiable evidence of such interactions?
   (b) How can a teacher at school A provide a license to school B to share her lecture slides to their students with the assurance that she will earn some royalties based on students' interaction with her lecture slides?
(2) How can students generate and share learning materials with their peers across different schools with IPRs protection? E.g.
   (a) A student at school A can generate useful notes or quizzes that are useful to other students. How can students become aware, request access and rate such con-

1 Graduate School of Informatics, Kyoto University, 36-1 Yoshida-Honmachi, Sakyo-ku, Kyoto 606-8501, Japan.
2 Academic Center for Computing and Media Studies, Kyoto University, Yoshida-Nihonmatsu, Sakyo-ku, Kyoto 606-8501, Japan.
a) ocheja.ileanwa.65s@st.kyoto-u.ac.jp
b) flanagan.brendanjohn.4n@kyoto-u.ac.jp
c) hiroaki.ogata@gmail.com

tents in favor of the original author?

(3) For companies, other learning organizations, and publishers, how can we establish a trusted and transparent network where these actors can co-exist and provide a wide pool of educational resources to students? E.g.
   (a) Like e-commerce platforms with multiple sellers, is it possible to have publishers, and content creators from different learning platforms including MOOCs provide their learning materials to students who wish to subscribe with no single school controlling the entire network?

1.2 BOLL as an e-Learning Marketplace

We provide solutions to the above problems by extending the framework for a blockchain-based learning analytics platform proposed in [11] and implemented in [5] as a Blockchain of Learning Logs (BOLL). BOLL is a decentralized platform that enables logical movement of students and their academic records from one institution to another. Different from certificates or transcripts issuing systems, BOLL provides a mechanism to share learning logs of students on the various learning tools they interacted with while studying at different institutions. The privacy of students' data is also ensured through the installed smart contracts and the private-public key architecture of the Ethereum blockchain on which BOLL is built. We make the following contributions to BOLL:

1.2.1 Learning Materials Publishing Tools Integration

To make it possible to publish learning materials on BOLL, we integrate into BOLL features that allow for learning material publishing, usage visualization, and storage. Just like the Learning Record Store (LRS), a Data Depository Server (DDS) for storing actual learning materials can also be attached to BOLL. To keep the DDS from unauthorized access, we also integrate a SecureBox that ensures all access requests are verified with the blockchain to ensure appropriate signature and compliance before serving the requested resource.

1.2.2 Smart Contracts for IPR Protection, Learning Materials Usage, Review, Rating and Collaborative Authoring

We represent intellectual rights to learning materials as smart contracts which authors and users of their work must agree to. We also provide various types of smart contracts for different scenarios ranging from one-time access authorization to multi party dependent policies. Authors can also receive reviews and ratings from users about their works or policies.

1.2.3 Decentralized Marketplace for Learning Materials

With more learning providers joining BOLL and providing more learning materials through their various publishing tools, we integrate into BOLL a marketplace to help users easily locate these learning materials.

The rest of this paper is organized as follows. The next section reviews related works and how our idea differ from existing solutions. This is followed by the section on our proposed framework and its components. Our discussions and ideas to solving identified problems and potential challenges are provided in the discussions section. Finally, we conclude this paper and provide potential directions for future work.

2. Related Work

There have been many previous works on the need to protect IPRs in a digital world including [1, 2, 4, 6, 7]. The paper [4] discussed the use of policing, litigation, restricted sharing, and the use of Digital Rights Management (DRM) elements including content encryption, keys, passwords, and third-parties for tracking usage to ensure non-violation of digital rights. On using technology to achieve access control to digital assets, Anderson et al. [10] proposed an eXtensible Access Control Markup Language (XACML) geared towards achieving more usability of digital assets over a broad spectrum of applications and to also ensure security policies defined by asset owners are adhered to. To achieve this, XACML provides a request and response format for interacting with the policy system and how to interpret such policies. A Policy Decision Point (PDP) evaluates applicable policy and renders authorization decision while a Policy Enforcement Point (PEP) performs access control by making decision requests and enforcing authorization outcomes.

Lorch, Proctor, Lepro, Kafura and Shah [9], demonstrated how XACML can be used by distributed systems to achieve a more robust access control. XACML is observed to overcome the limitations of Shibboleth [12] such as Shibboleth's dependence on htaccess files which are inherently deficient and not so easy to share in arbitary locations [9]. However, XACML and the implementation in [9] does not provide a mechanism for engendering trust between two or more potentially distrustful parties without the need for a central authority to act as a mediator. To solve the problem of lack of trust and eliminate the need for a third-party, Zhu et al. [13] proposed a Transaction-based Acces Control (TBAC) assets management system on blockchain which is fundamentally built on an Attribute-based Access Control (ABAC) model [14]. Using the Bitcoin blockchain, Zhu et al. showed how a digital asset can be escrowed on the blockchain and protected with policies defined in state functions.

While the ideas proposed by Zhu et. al. are similar to ours, we find their work limited in handling third-party scenarios identified in our research questions stated earlier. Also, while the goal of an asset management system might be to control access and ensure policies are not abused, we consider the case of students learning, sharing and accessing learning resources in digital forms to be peculiar and thus, should be handled differently. These papers [15, 16] also identified the possibility of using the blockchain technology to manage intellectual property but focused its concern on using the blockchain to manage journal management workflows.

The Blockchain of Learning Logs (BOLL) proposed in [5] enables the realization of lifelong learning logs for students as they move from one learning environment to another. Using the blockchain technology, BOLL ensures that students' privacy is protected through permissions defined in installed smart contracts. The BOLL framework forms a fundamental background for our work. Our proposed framework allows broad auditing by concerned parties on the network and also permits digital content owners to decide how their contents from the DDS are served to other users in order to facilitate better policy violation tracking. Also, to improve learning outcomes, we introduce a mechanism for users to rate and recommend useful contents to one another.

3. Proposed Framework

Figure 1 shows our proposed framework for enabling a decentralized e-learning marketplace for managing authorship and tracking access to digital contents on BOLL. We refer to our proposed system as BOLL Marketplace (BOLL-M). BOLL-M comprise of two groups of users; authors and users. Authors refer to actors on BOLL-M who own intellectual rights to learning materials made available in the marketplace. While users refer to members of the BOLL network who wish to access learning materials made available in the market and/or organizations that provide sponsorship for students to access learning materials (e.g. a government education ministry or other funding organizations). It is important to state that a student or teacher on BOLL-M can also be an author of a learning material in the marketplace. In this scenario, the student or teacher can rely on the learning material publishing tool made available to them by their institution. For publishers who do not belong to an academic institution, it is required for them to be authorized by the BOLL Consortium proposed in [5]. After such an authorization is acquired, the publisher can setup a node on the BOLL network as show in figure 2. We will now describe each of the components shown in figure 1.

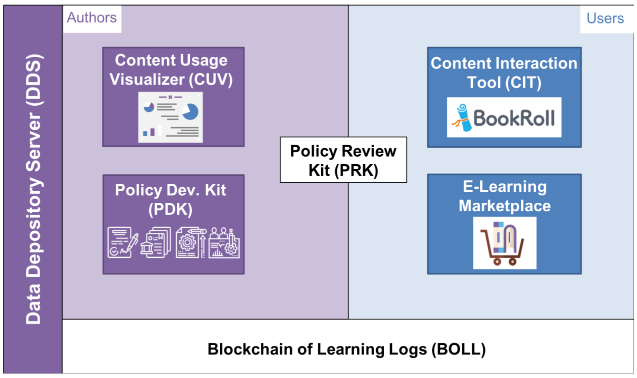

Fig. 1 Decentralized e-learning marketplace

3.1 Policy Development Kit (PDK)

To enable appropriate use of learning materials on BOLL-M, it is necessary to define policies that accessors should comply with. We represent these policies as state transition functions in the smart contracts. Due to the technical skills required to write smart contracts, we provide multiple templates as a PDK which authors can choose from, adapt to their use case and install on BOLL to protect access to their learning materials. We represent these smart contracts in four broad categories.

3.1.1 One-time Signatory Policy (OSP)

This refers to smart contracts that can be installed once and contain clauses on how a learning material can be accessed and used with the permission of the author. When an OSP is issued on BOLL-M, it is irrevocable and the issuer either grants a limited or lifetime access to a learning material depending on the duration specified. An example of a useful application is where students are given a one-time limited access to a professional or degree examination provided by another organization.

3.1.2 Dual Party Signatory Policy (DPSP)

This is a revocable version of OSP where two parties can agree or disagree on the terms of access to a learning material. In a DPSP, terms of access can be modified by the issuer and such modified version becomes valid only when the accessor of the learning material agrees to the new terms. DPSP is useful in scenarios where an author maintains a continuously improved version of a learning material (e.g. lecture slides being updated regularly) and does not wish to create an entirely new version with the new changes. Although, smart contracts once installed are immutable, we achieve versioning of terms of access by allowing a bi-directional pointer between the initial DPSP and the new DPSP. The initial DPSP becomes invalid only when the user accepts the new DPSP. The user will be unable to access the learning material unless they accept the new terms.

3.1.3 Multi Party Signatory Policy (MPSP)

The MPSP is a collaboration enabled smart contract that allows multiple parties to determine the conditions for accessing a learning material. To enable multi party arbitration, MPSP starts off with the proposed clauses of the originating party. Another party can review these proposals and either refuse or accept them by invoking the state transitions functions contained in the initial MPSP. When the arbitration requires only two parties, a new MPSP is issued if the second party accepts the clauses otherwise the initial MPSP is invalidated. If the MPSP requires more than two parties, the smart contract becomes invalid if a simple majority disagrees with the stated terms. In a case where a tie occurs, the parties can propose one party whom they think should be the final arbiter. This party is then given the ability to override all votes and either accept or deny the approved installation of the MPSP. For instance, we find the MPSP useful in a three-party scenario where one party owns and provides the learning material (e.g. publisher), the second party pays for the learning material (e.g. government) and the third party is the consumer of the learning material at no cost (e.g. students). This solves the particular problem where an organization sponsors access to a learning material on behalf of the students. The tie breaker is useful in a case where the sponsoring organization is unable to ascertain the usefulness of a learning material to the student. In this case, both the sponsoring organization and the author can delegate the student to adjudge whether they find such learning material useful or not.

3.1.4 Discovery Policy (DP)

In order for an author or a publisher's learning material to show in the e-learning marketplace on BOLL-M, the author is required to install a DP smart contract. This contract contains a basic information about the learning material such as title, date published, version, description, applicable smart contracts (at least one of OSP, DPSP, MPSP). Because the DP smart contract does not contain the actual learning material or pointers to it, it is publicly available to anyone on the network to access but not modify. Only the authors can modify the DP smart contract as required should they require to make any changes to the original terms or attributes. It should be noted that updating the associated smart contracts applicable to a learning material does not result to inval-

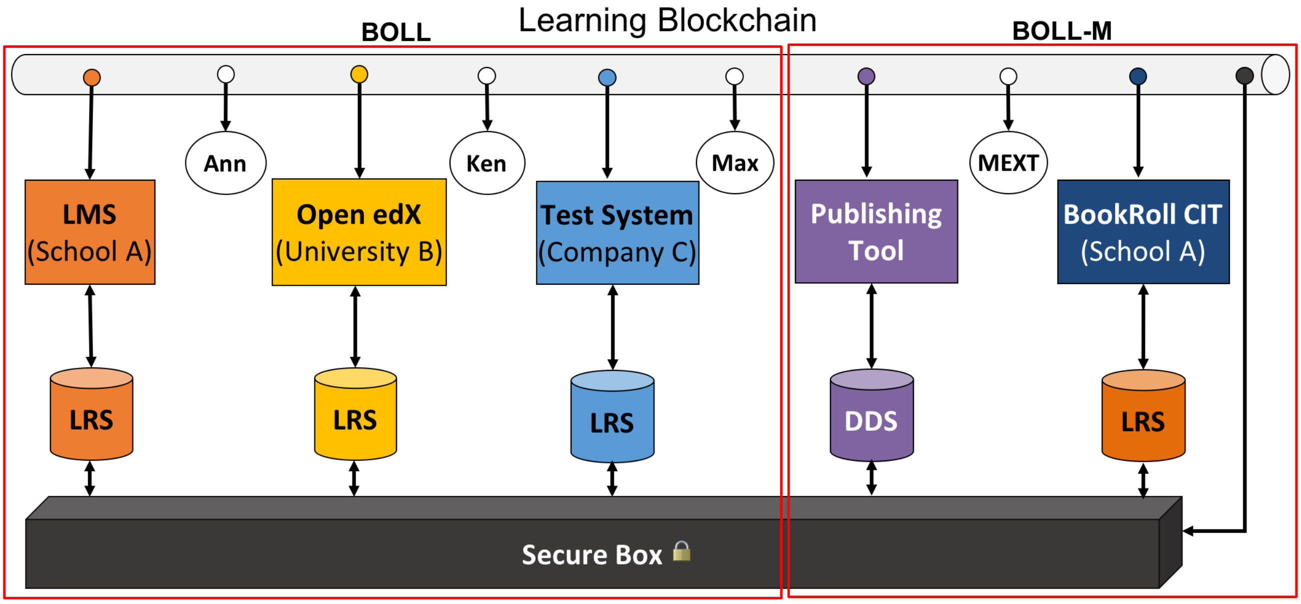

Fig. 2 Decentralized e-learning marketplace on BOLL

idation of the previously granted rights. To invalidate any previous access authorization, the procedures of the initial smart contract used to protect that learning material should be followed.

3.2 Policy Review Kit (PDK)

The PDK contains a set of useful tools for reviewing proposed as well as installed policies or smart contracts. This include policy modifying tools like acceptance, refusal or arbitration, and learning material rating tools. The policy modifying tools are provided to ensure that other parties understand the defined terms before accepting them. Learning material rating tools are useful for helping students find contents that might be appropriate for different scenarios based on the perception of their peers or teachers.

3.3 Content Usage Visualizer (CUV)

We propose an interface for authors and sponsors to visualize the interactions users have made with their learning materials. Since all transactions on the blockchain are written to a public ledger whose contents are immutable, we realize the CUV by querying this public ledger. However, because some functions in the installed smart contracts do not modify state and thus do not lead to transactions, we consider it a necessity that all request to view a learning material should invoke at least, a payable transaction so that access histories can also be written to the ledger. This can be achieved by mandating that all functions used to check access authorizations before returning a learning material should write on the ledger a message signed by the accessor. Also, we restrict what can be shown in the visualizer to only those attributes specified in the installed smart contracts and already agreed to by the accessor. For real-time notification of interactions, we recommend the registration of event observers on the BOLL node.

3.4 Data Depository Server (DDS)

Due to the time it takes to process transactions on the blockchain for even small-size data, we do not recommend storing the learning materials on the blockchain. We recommend that authors or publishers should store their learning materials on a DDS. For students and teachers who might not be able to setup the publishing tool shown in figure 2 (Consisting of CUV, PDK, and a part of PRK), we envisage that their schools would setup a shared publishing tool and a DDS. The DDS is connected to the SecureBox proposed in [11] and all requests sent to the DDS are verified with BOLL through the SecureBox.

3.5 E-Learning Marketplace

The e-learning marketplace is an interface that lists all learning materials published on BOLL-M. For an author's learning material to show in the marketplace, it is required that the author should install a DP smart contract. This contract can be retrieved from the PDK and adapted to the author's use case. An author may also specified that their learning material can be discovered in the marketplace by only selected users. Once a user identifies a learning material which they wish to access from the marketplace, they can review the required policy and decide on how to proceed. If the user finds the policy unfavorable, refusing to accept it does not trigger any other procedure. But if the user finds the policy acceptable and accepts the terms, the access authorization process is triggered depending on the type of smart contract in question. Also, within the marketplace, users who have accepted a particular learning material's terms can also rate it.

3.6 Content Interaction Tool (CIT)

To ensure that intellectual rights of authors are not violated, we recommend that the tool for viewing escrowed learning materials, here referred to as Content Interaction Tool (CIT), should be connected to BOLL. In figure 2, we use BookRoll, a digital book reader as our CIT. BookRoll traditionally logs user interactions with digital books including bookmarking, highlights, page turns, etc. We consider these interactions enough to know when a user accesses an escrowed learning material. For recording a simple interaction on BOLL-M, one can simply register an access event when the content is being served for the first time. In a case where monitoring more interactions is desired, we can listen to specific events of the CIT. As BookRoll stores user logs on a Learning Record Store (LRS), it is possible to listen to page turn events and subsequently notify BOLL-M of these interactions. We note that monitoring of the user's interactions can be an invasion of privacy. Hence, we recommend that this should only be done according to the terms of the smart contracts.

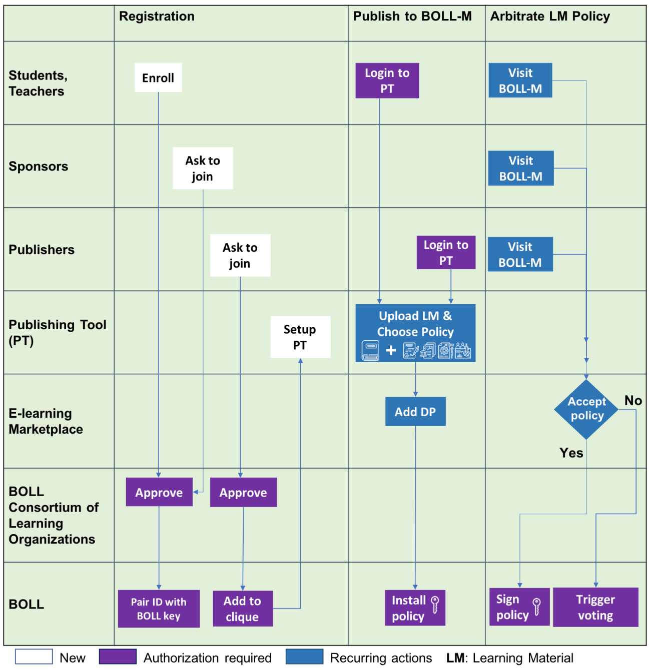

Fig. 3 A simulation of registration, publishing and arbitration processes on BOLL-M.

In figure 3 above, we simulate the registration, publishing and policy arbitration processes on learning materials shared on BOLL-M. We show how various actors such as students, teachers, sponsors, publishers and other learning organizations can regulate how different learning resources can be shared on BOLL-M. For students and teachers to join BOLL-M, they are required to follow the same procedure required for enrolling on BOLL, i.e. they should enroll in an institution that is already a member on BOLL. Sponsors are also required to enroll through the schools they wish to sponsor. In a case where a sponsor has already joined BOLL by sponsoring at least one school, that sponsor can easily issue a message signed with their private key stating that they wish to sponsor another school on the network. Publishers can only join the network when their request is approved by the BOLL consortium. Upon approval, the publisher can then setup a BOLL node and a publishing tool for managing and publishing their learning materials on BOLL. To publish on BOLL, all authors (including students, teachers and publishers) should do so from a publishing tool and upload the learning material on a BOLL-connected DDS and specify the appropriate policies. For a learning material to show up in the e-learning marketplace, the author is required to add a DP smart contract before writing these records on the BOLL. For arbitrating policies specified on learning materials, concerned parties have to visit BOLL-M to view such learning materials, review the attached policies and then decide whether to append their signature to it or not. If they choose to disagree with the policy and such refusal satisfies the minimum requirement for dispute resolution, a voting process is triggered on the BOLL network and all parties involved are notified.

4. Discussion

In this section, we present some questions and ideas that have made solving this problem interesting.

4.1 What Should Authors Track?

With the growing privacy concerns within the digital environment, it is necessary to address what authors are able to track about users' interactions with their learning materials. By default, authors should only be aware of direct access such as a request to serve a given learning material. But in a case where detailed interactions such as page views are required to calculate cost, users should be informed during the policy review phase by selecting an appropriate smart contract. In turn, the CIT can then query BOLL-M before feeding forward any interaction events to the concerned smart contracts if required.

4.2 Collaborative Content Authoring

We have shown how the MPSP smart contract can be used to foster collaborative policy formulation. In a situation where two or more authors want to independently improve a particular learning material, BOLL-M should provide a medium for such collaboration. This can be achieved through a version control mechanism with each author ascribing a particular smart contract to their own section. A simple approach might be to consider these versioned sections as either preceding or succeeding learning material depending on the changes time-line.

4.3 Rewarding Intellectual Contribution

When students achieve certain milestones while interacting with a learning material, it is often deemed necessary to reward their efforts. Similar to computer games where efforts are rewarded, we find it appealing to integrate such rewards into BOLL-M. Students who interact with certain learning materials, contribute useful learning materials and/or solve quiz problems could be rewarded with points. These points can then be traded for other learning materials or digital assets on BOLL or on other platforms.

5. Limitations

We also acknowledge the following limitations and suggest some methods that can be adopted in tackling them.

5.1 Tracking Access Outside CIT

One common problem faced when sharing learning materials online is the inability to track "detached" learning materials. Detached learning materials are learning resources that have been illegally reproduced by a user who has access to them. When such reproduction occurs, the reproduced version is no longer within the control of BOLL-M to manage its authorship rights. While this is a challenge, we recommend the development of interactive features within the CIT that renders any illegal reproduction unattractive and deficient in serving the original purpose.

5.2 Content Quality

We consider the quality of learning materials to be a major determinant of its usefulness. In our proposed framework, we assume that authors and/or publishers will provide high quality learning materials. We propose the use of the ratings provided by the users through the PRK in determining how publishers are regulated on the network. In a case where students generate learning materials and wish to share on BOLL-M, we recommend their institutions to provide an intermediate review on the publishing tool provided to the students.

5.3 Detecting Plagiarism

To detect plagiarism on BOLL-M, it is required to analyze contents of submitted learning materials. While we consider this to be outside the scope of our current framework, we suggest that users should take advantage of the PRK and report suspected plagiarized works through it. By using this decentralized approach of reporting intellectual theft, the network can actively detect plagiarism and further adjudicate on the next line of action. Also, adjudicating plagiarism can be integrated into smart contracts to ensure immediate effect upon discovery.

6. Conclusion and Future Work

In this work, we proposed a framework for enabling decentralized e-learning marketplace on BOLL. This framework facilitates managing of intellectual rights, tracking access and fostering collaboration between different users, authors and publishers. We described how authors can define terms of use on their learning materials and how students can access these learning materials on the blockchain where their privacy is not violated. Alongside other smart contracts, MPSP smart contract plays an important role in facilitating collaborative policy formulation, learning material sponsorship and verifiable proof of learning material consumption. We have also presented some ideas on how to tackle some identified problems such as ensuring good content quality, detecting plagiarism, fostering content co-authoring and rewarding efforts. Future work will be focused on providing a concrete implementation of this framework on BOLL towards enabling BOLL as a wide-reaching system.

Acknowledgment

This work was partly supported by JSPS Grant-in-Aid for Scientific Research (S)16H06304 and NEDO Special Innovation Program on AI and Big Data 18102059-0.

References

[1] Kahin, B. and Varian, H. R.: *Internet publishing and beyond: The economics of digital information and intellectual property*, MIT Press (2000).

[2] Chuang, J. C. and Sirbu, M. A.: *Network delivery of information goods: Optimal pricing of articles and subscriptions*, Proc. Internet Publishing Beyond: Econom. Digital Inform. Intellectual Property. Kennedy School of Government, Harvard University Cambridge, MA. (2000).

[3] May, C.: *World Intellectual Property Organization (WIPO): Resurgence and the Development Agenda*, Routledge (2006).

[4] Foroughi, A. and Albin, M. and Gillard, S.: *Digital rights management: a delicate balance between protection and accessibility*, Journal of information science (2000).

[5] Ocheja, P. and Flanagan, B. and Ogata, H.: *Managing Lifelong Learning Records Through Blockchain*, Research and Practice in Technology Enhanced Learning. (In Press).

[6] National Research Council and others: *The digital dilemma: Intellectual property in the information age*, National Academies Press (2000).

[7] Liu, Q. and Safavi-Naini, R. and Sheppard, N. P.: *Digital rights management for content distribution*, Proceedings of the Australasian information security workshop conference on ACSW frontiers. Vol. 21, pp.49–58. (2003).

[8] Goel, S. and Miesing, P. and Chandra, U.: *The impact of illegal peer-to-peer file sharing on the media industry*, California Management Review. Vol. 52, No. 3, pp. 6–33. (2010).

[9] Lorch, M. and Proctor, S. and Lepro, R. and Kafura, D. and Shah, S.: *First experiences using XACML for access control in distributed systems*, Proceedings of the 2003 ACM workshop on XML security. pp. 25–37. (2003).

[10] Anderson, A. and Nadalin, A. and Parducci, B. and Engovatov, D. and Lockhart, H. and Kudo, M. and Humenn, P. and Godik, S. and Anderson, S. and Crocker, S. and others: *extensible access control markup language (xacml) version 1.0*, OASIS. (2003).

[11] Ocheja, P. and Flanagan, B. and Ogata, H.: *Connecting Decentralized Learning Records: A Blockchain Based Learning Analytics Platform*, In LAK '18: Proceedings of the 8th International Conference on Learning Analytics and Knowledge. pp. 265–269. (2018).

[12] Cantor, S. and Scavo, T.: *Shibboleth architecture*, Protocols and Profiles. Vol. 10, p. 16 (2005).

[13] Zhu, Y. and Qin, Y. and Zhou, Z. and Song, X. and Liu, G. and Chu, W. C.: *Digital Asset Management with Distributed Permission over Blockchain and Attribute-Based Access Control*, 2018 IEEE International Conference on Services Computing (SCC). pp. 193–200. (2018).

[14] Hu, V. C. and Ferraiolo, D. and Kuhn, R. and Friedman, A. R. and Lang, A. J. and Cogdell, M. M. and Schnitzer, A. and Sandlin, K. and Miller, R. and Scarfone, K. and others: *Guide to attribute based access control (ABAC) definition and considerations (draft)*, NIST special publication. Vol. 800, No. 162. (2013).

[15] Janowicz, K. and Regalia, B. and Hitzler, P. and Mai, G. and Delbecque, S. and Fröhlich, M. and Martinent, P. and Lazarus, T.: *On the prospects of blockchain and distributed ledger technologies for open science and academic publishing*, Semantic Web. Preprint pp. 1–11. (2018).

[16] Hoffman, M. R. and Ibáñez, L. and Fryer, H. and Simperl, E.: *Smart Papers: Dynamic Publications on the Blockchain*, European Semantic Web Conference. pp. 304–318. (2018).