Blockchain-based Paper Submission System for Author Nonrepudiation and Plagiarism Checking

Shin-Ting Wu[1], Yi-Hua Chen[2,1], and Po-Chun Huang[1]

[1]Department of Electronic Engineering, National Taipei University of Technology, Taipei, Taiwan, ROC

[2]Department of Computer Science, National Tsing Hua University, Hsinchu, Taiwan, ROC

Received xx mm 201x; received in revised form xx mm 201x; accepted xx mm 201x

Abstract

With the increasing events of academic ethic violations, how to ensure academic integrity has become a highlighted issue among all academic fields. For example, how to ensure that all co-authors have agreed the submission of a research work to a conference or journal is an important issue. Meanwhile, how to ensure that reviewers and journal editors cannot plagiarize the submissions under review is also an important issue. On the positive side, due to the ethical rules of IEEE, authors need an open platform to check whether their submitted manuscript contains any sequence of words that appeared in prior literature. In this work, we shall focus on common academic ethic rules, and propose a blockchain-based system to detect or prevent from the violations of academic ethical rules. To verify the feasibility and efficacy of the proposed system, a prototype system is under implementation as well.

Keywords: academic ethics, blockchain, nonrepudiation, plagiarism checking

1. Introduction

Recently, more and more violation events of academic ethics have been discovered in various forms of academic publications, such as conference papers, journal articles, and even monographs [41, 42]. The cases of violations of academic ethics also become more diversified, as studied by many prior work [41, 42, 43]. Although educating new researchers to equip them with the correct sense of academic ethics is a key task, another important reason might fall on the current incomplete and insecure processing procedure of academic publications. For example, existing paper submission systems cannot effectively verify whether all authors agree the submission of a collaborated research work [41, 49, 50]. That is, an author might deny that he or she has been involved in the collaboration of some questionable research work. What is worse, some well-known authors might be maliciously added to the author list without their prior consents [16, 41]. In other words, the *nonrepudiation of authorship* [41] should be inherently guaranteed by the submission procedure. In another example, once a manuscript is submitted to a peer-reviewed conference or journal, the secrecy of the contents of the manuscript no longer preserves, and malicious reviewers (in some rare cases, editors) might be able to plagiarize the submitted manuscript and submit the manuscript to other places, as if they were the original authors. The *authentication of authorship* [41] is thus an important technical issue as well. It is therefore in an urgent need to enhance the existing paper submission and processing procedures to automatically avoid such academic ethical problems without human intervention.

Providing a shared ledger among a number of peers that do not completely trust each other, the blockchain technologies have observed tremendous advances in various application scenarios [27, 47, 51, 52, 54]. For instance, blockchains can be used as an electronic laboratory book that keeps the research logs, which are encrypted using public–private key encryption systems. As the original researcher can show that he or she can decrypt an encrypted log using his or her own key, the originality of research results can be validated, thereby avoiding potential arguments about the original authorship [55]. Similar applications can also be used to protect the originality (earlier inventions) and integrity (against tampering) of important shared data, such as intellectual properties [52] and medical records [51].

The technical contributions of this work are summarized as follows. First of all, we propose a new manuscript management system architecture and the accompanying paper submission protocols, so as to overcome the difficulty to protect submitted, but not yet accepted manuscripts by blockchains in the midway of the review process. After that, we enable a significant characteristic that all co-authors must agree before a manuscript can be submitted to a conference or journal. On the other hand, a coauthor cannot be added to the author list without his or her prior agreement, and an author on the author list of a submitted manuscript cannot deny that he or she was not involved in the research work. With a distributed shared ledger based on blockchains, many cases of academic ethical rule violations can be automatically detected and prevented without any human interventions.

The rest of this paper is organized as follows. First, Section 2 investigates on several case studies of academic ethic rule violations and motivates this work. After that, in Section 3, a novel paper submission system and the accompanying paper submission protocol based on blockchains are proposed to automatically prevent from several common cases of academic ethic rule violations. The survey and comparison of related work are given in Section 4. Section 5 is the conclusion and future work.

2. Motivational Observations on Academic Ethic Rules

This work is motivated by the observation that intellectual properties and academic innovations nowadays might be violated in the submission and review process of a paper. In this section, several typical cases of academic ethic rule violation are investigated, based on which we shall seek for possibilities to exploit the blockchain technology to protect academic contributions made.

CASE 1. Paper submission without common agreement of all authors

As discussed in some prior arts [16, 41], some authors might add irrelevant authors to the author list without prior consent of all authors, which is obviously a violation of academic ethic rules. In another case, it is possible that some authors of a paper think that the manuscript has been ready for submission, while the other do not. Such a manuscript should not be submitted because not all authors have reached a common agreement that the manuscript is ready for submission.

CASE 2. “Explicit” parallel submissions

In this work, we define *“explicit” parallel submissions* as the case where two manuscripts with (partially or completely) overlapped author lists and identical syntactical constructs such as sentences or paragraphs are submitted to the same or different conferences or journals. On the other hand, *“implicit” parallel submissions* are defined as the case where two manuscripts with overlapped author lists and identical or very similar technical contributions or academic innovations. Nevertheless, both flavors of parallel submissions are prohibited by academic ethic rules. In this work, we primarily focus on the explicit parallel submissions because dealing with the latter requires *natural language processing* techniques for semantic analysis and is beyond the scope of this work.

CASE 3. “Explicit” plagiarisms of a submitted manuscript by reviewers or editors

The case of “explicit” plagiarisms is similar to that of “explicit” parallel submissions, except for that explicit plagiarisms often refer to the case where a latter submission contains identical syntactical constructs to a previously accepted paper. The case for implicit plagiarisms is similar. However, unlike parallel submissions, there is a special case of plagiarisms, which is not considered as plagiarisms and thus allowed. If a paper is previous accepted by a conference, it can be extended by a (partially or completely) overlapped set of authors as a journal submission, provided that (i) the extension relationship must be clearly indicated in the journal submission (usually in the footnote of the first page), (ii) the journal submission must be clearly differentiated from the original conference paper by a *Summary of Differences* report, which should be prepared by the authors and sent along with the conference paper to the journal editors and reviewers for reviewing, and (iii) there should be at least 30%–100% of technical differences between the conference and journal versions. Such an exception in the academic ethic rules could further complicate the plagiarism checking process, as addressed in better details in the subsequent sections.

With the key observations over common violations of academic ethic rules, this work is motivated to exploit the blockchain technologies to maintain a verifiable and reliable platform to protect academic innovations from careless or intentional plagiarisms. In particular, our main objective is to enhance existing tools and procedures used to handle the submission of academic papers, so as to effectively and efficiently detect and even prevent from academic ethic rule violations.

3. Utilizing Blockchain Technologies for the Protection of Academic Ethic Rules

3.1. A Novel Manuscript Submission Protocol for Author Identity Validation and Non-repudiation

The high-level architecture of the proposed paper submission system is briefed as in Fig. 1. There are three major peers involved in the paper submission process, namely, the *authors* (Fig. 1, left), the *paper submission host* (Fig. 1, middle), and the *editor and reviewers* (Fig. 1, right). The paper submission host is assumed authenticated by trusted academic organizations such as IEEE, ACM, or USENIX, and is considered not malicious. On the other hand, each author and reviewer could attempt to violate academic ethical rules for their own benefits, as described in the previous sections. For the clarity and precision of discussion, we concentrate on a manuscript collaborated by m authors, who are numbered as $1, 2, \dots, m$, respectively. The cleartext of the to-be-submitted manuscript is denoted as N. With commodity public–private key encryption schemes such as RSA algorithm [56], let us denote the public and private keys of author i as e_i and d_i, respectively. The ciphertext obtained by encrypting some message N with key d_i is denoted as (N, d_i), while the cleartext obtained by decrypting some ciphertext (N, d_i) with public key e_i is similarly denoted as $\left((N, d_i), e_i\right)$.

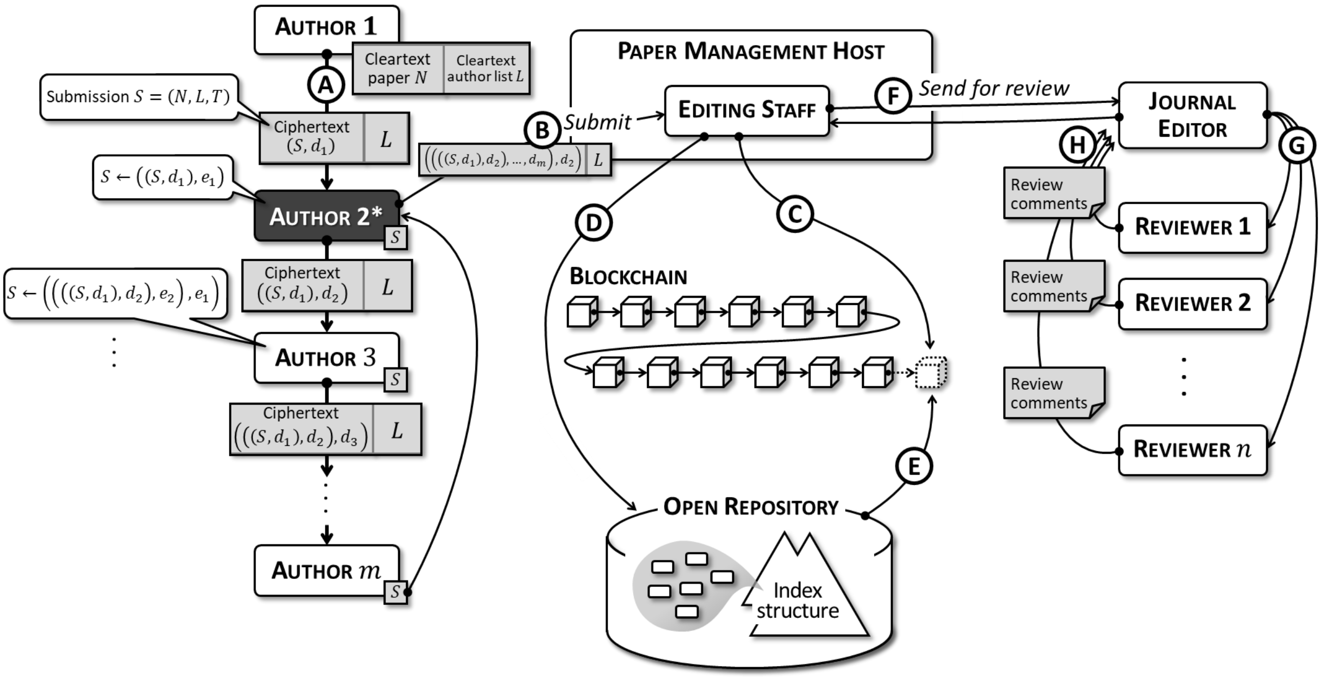
Author 1
Cleartext paper N
Cleartext author list L
A
Submission $S = (N, L, T)$
Ciphertext (S, d_1)
L
$S \leftarrow ((S, d_1), e_1)$
Author 2*
S
Ciphertext $((S, d_1), d_2)$
L
$S \leftarrow \left(\left(\left(((S, d_1), d_2), e_2\right), e_1\right)\right)$
Author 3
S
Ciphertext $\left(((S, d_1), d_2), d_3\right)$
L
Author m
S
B
Submit
$\left(\left(\left(((S, d_1), d_2), \dots, d_m\right), d_2\right)\right)$
L
Paper Management Host
Editing Staff
F
Send for review
Journal Editor
C
D
Blockchain
E
Open Repository
Index structure
H
G
Review comments
Review comments
Review comments
Reviewer 1
Reviewer 2
Reviewer n

Fig. 1. System architecture. The author marked with asterisk *, *i.e.*, Author 2 in this example, is the corresponding author.

The proposed paper submission process associated with the above architecture is classified into four major phases, particularly the *pre-submission*, *submission*, *review*, and *post-review* phases. In the pre-submission phase (Fig. 2), all authors must reach a common agreement that the manuscript can be submitted. This is done by a *serial polling process* through the first to the last author of the manuscript (Step Ⓐ). In the polling process, each author must verify the contents of the to-be-submitted manuscript, as well as whether his or her corresponding metadata are correct in the manuscript. Specifically, in the beginning, Author 1 uses his or her own private key d_1 to encrypt the to-be-submitted data S, which contains the cleartext N of the manuscript, the author list L, and a timestamp T. The timestamp T keeps the time point at which the submission process is initiated. After that, Author 1 sends the encrypted result of S, namely (S, d_1), to the next author. Author 2 then uses the public key e_1 of Author 1 to decrypt the ciphertext (S, d_1) to get the cleartext $S = (N, L, T)$, and verifies whether the contents of the manuscript and other metadata are correct. If e_1 cannot correctly decrypt (S, d_1), the contents of the manuscript are incorrect or the author lists in cleartexts and ciphertexts do not agree, the submission procedure fails. Otherwise, Author 2 will further encrypt (S, d_1) using his or her private key d_2 into $\big((S, d_1), d_2\big)$, and send the resulted ciphertext $\big((S, d_1), d_2\big)$ to the next author in the list, and the same actions will be repeated until all authors have agreed the submission, or the process is aborted. Once all authors agreed the submission, the final encrypted paper $\Big(\big((S, d_1), d_2\big), \ldots, d_n\Big)$ will be sent to the corresponding author, Author 2 in this example, who will then submit the manuscript to the paper management host (Step Ⓑ). As astute readers might point out, during this serial polling process, any single author cannot submit the paper on behalf of others, because he or she does not have the private key of other authors for manuscript encryption. Please also note that the cleartext of the author list must also be sent to every author, along with the encrypted file of manuscript and author list, for verification purposes.

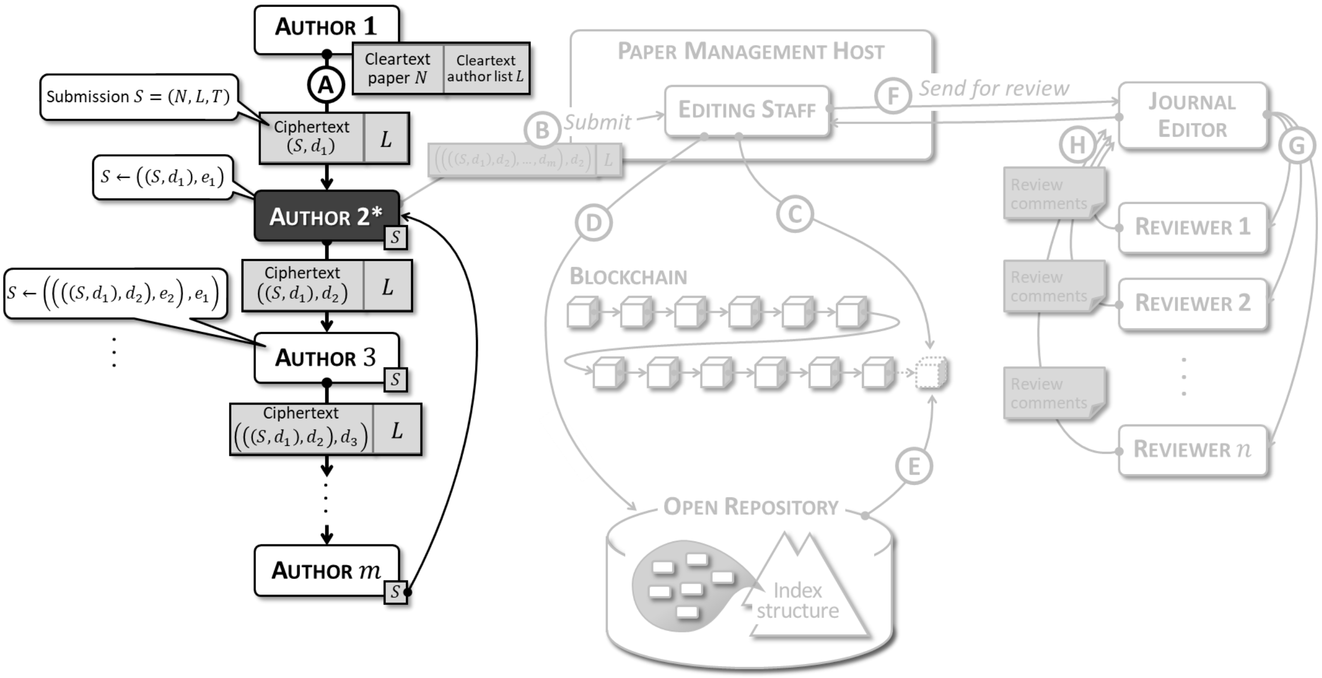
AUTHOR 1
Cleartext paper N
Cleartext author list L
A
Submission $S = (N, L, T)$
Ciphertext (S, d_1)
L
$S \leftarrow \big((S, d_1), e_1\big)$
AUTHOR 2*
S
Ciphertext $\big((S, d_1), d_2\big)$
L
$S \leftarrow \Big(\big(((S, d_1), d_2), e_2\big), e_1\Big)$
AUTHOR 3
S
Ciphertext $\Big(\big((S, d_1), d_2\big), d_3\Big)$
L
AUTHOR m
S
PAPER MANAGEMENT HOST
B
Submit
$\Big(\big(((S, d_1), d_2), \ldots, d_m\big), d_2\Big)$
L
EDITING STAFF
F
Send for review
JOURNAL EDITOR
H
G
Review comments
REVIEWER 1
Review comments
REVIEWER 2
Review comments
REVIEWER n
D
C
BLOCKCHAIN
E
OPEN REPOSITORY
Index structure

Fig. 2. The pre-submission phase.

In the submission phase (Fig. 3), the corresponding author will submit the paper encrypted with the private keys of to the paper management host. The duties of the paper management host are to check the integrity of author list and potential doubts of plagiarisms. To realize plagiarism checking, the submitted manuscript will be decomposed into syntax units such as sentences, whose hashed values will then be maintained in a public repository (Step Ⓓ). If any sentence of a newly submitted manuscript matches the hashed value of any sentence of previous manuscripts logged in the blockchain, the newly submitted manuscript will be considered with the doubts of plagiarisms (Step Ⓒ). (To avoid *false positives* where innocent manuscripts are identified with plagiarisms, we ignore very short sentences or frequently-used proverbs here.) To prevent the stored hashed values from being tampered, the hashed value of all hashed values of sentences will be added as a transaction to the blockchain (Step Ⓔ).

Once the manuscript enters the review phase, it will be sent to a technical committee member of conferences or an associated journal editor (Step Ⓕ of Fig. 4), who would then assign the manuscript to multiple reviewers (Step Ⓖ). After the reviewers completed the review, the review comments will be sent back to the paper management host for the final decision (Step Ⓗ). Despite of the final decisions, in the last post-review phase, the hashed value of each sentence of the review comments could be maintained by the open repository as well. This is to guarantee the integrity of the previous review comments, which are provided by authors to the new editors and reviewers when the manuscript was rejected and resubmitted. With the hashed values of previous review comments kept in the open repository, reviewers of the new submission can verify that the previous-round review comments have not been tampered by the authors. In addition, because the contents of the original manuscript under review will often be referred to in the review comments, only the hashed values of the review comments, instead of the comments themselves, are stored in the opera repository, so as to keep the original contents of the submitted manuscript secret. Here, please note that the journal editor cannot bypass the uploading of review comments and directly create transactions in the blockchain, because the blockchain can be *written* only by authorized paper management hosts, such as the technical program committee (TPC) members of authorized conferences. (The write privilege is open for TPC members only during the conference date.) On the other hand, everyone in the society can *read* the contents of the blockchain for verification purposes at any time, such as the monitoring of the review fairness of conferences and journals. Because the maintenance of the blockchain and open repository are done by the paper management host, but not individual editors or reviewers, editors and reviewers cannot plagiarize the contents of the submitted manuscript as their own work.

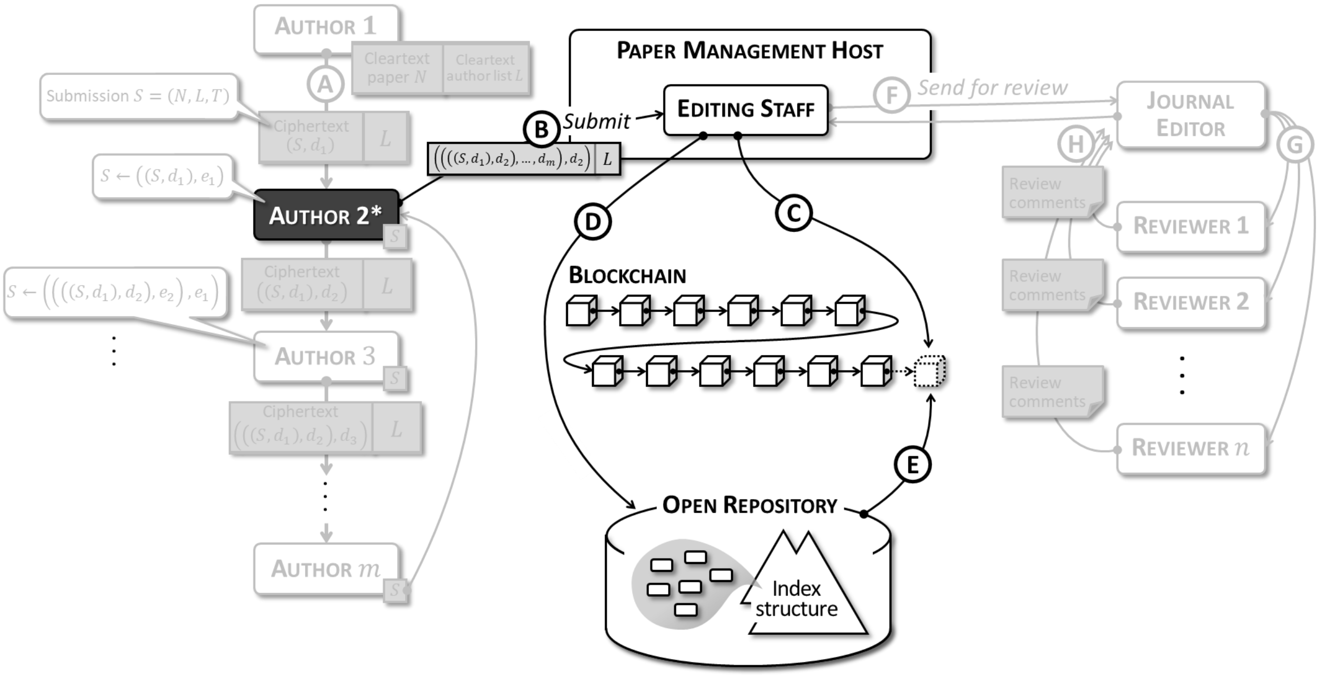

Fig. 3. The submission phase.

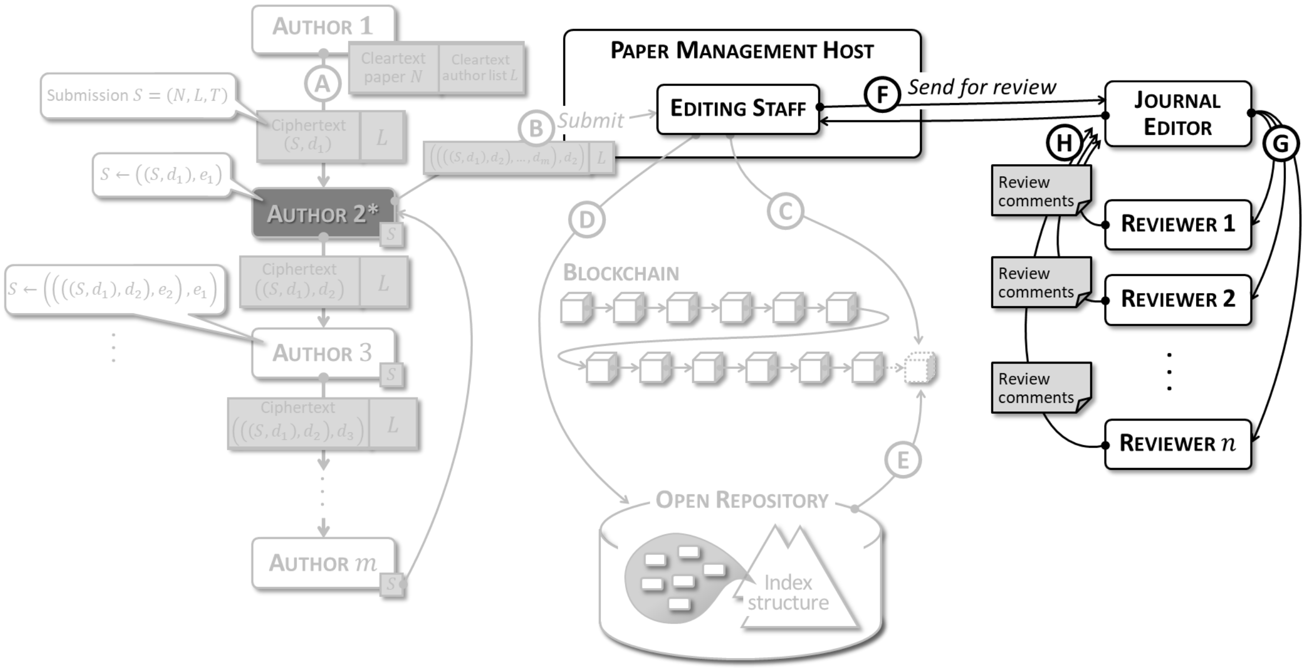

Fig. 4. The review phase.

3.2. Fine-grained, Blockchain-based Plagiarism Checking Strategy

Although various techniques have been proposed to analyze the similarity of articles for plagiarism checking [58, 59], a potential issue is that they must get full accesses to the original cleartext of the articles, which is often a proprietary service of academic publishers or organizations, such as ACM Digital Library [60], IEEE Xplore Digital Library [61], Springer [62], Elsevier [63], Oxford University Press [64], etc. Although some organizations such as USENIX provides free open accesses to the full texts of its conference proceedings [66, 67], the coverage of such open academic databases are still incomplete. A novel plagiarism checking method that can work with the proposed paper submission system and preserve the secrecy of unaccepted manuscripts is therefore in urgent need.

To realize the protection of the secrecy of unaccepted manuscripts, we propose to hash every language constructs, such as a *sentence* or *paragraph*, and maintain the hashed values of every sentence of all submitted manuscripts in the open repository. The secrecy is preserved because no cleartexts of the submitted manuscripts are explicitly stored in the system. In the meanwhile, whether fine-grained language constructs (such as sentences) or coarse-grained ones (such as paragraphs or even sections) should be used depends on the severity of plagiarisms. If copycats know how to reorganize the sentences in a paragraph to cheat the plagiarism checker, finer-grained (sentence-based) approach should be used. Although such a hash-and-compare strategy is straightforward, advanced algorithms such as *fully homomorphic encryption (FHE)* schemes [67, 68] can shed light on even smarter plagiarism checking while preserving the data secrecy, which is one of our important future work.

4. Related Work

The objective of the work is to protect academic ethical rules by a new paper submission/review protocol and blockchain-based paper submission system. In other words, we exploit the belief that many violation cases of academic ethical rules can be automatically eliminated by a better paper submission/review protocol and system.

The academic ethical rules have been a highlighted issue in all research areas. In some existing survey articles [16, 17], different types of violations of academic ethical rules are studied. For example, as the most severe case of plagiarism, complete plagiarism indicates the case in which some existing manuscripts are taken and submitted by someone other than the original researchers who performed the studies [41, 42]. On the other hand, *auto-plagiarism* or *self-plagiarism* is the case where someone plagiarizes his or her previous manuscript as a new submission [41, 43]. Furthermore, inaccurate authorship reflects two opposite subcases, where in one subcase some contributing authors do not get credits they deserve, and some irrelevant peers are accredited in the author list in the other subcase [16, 17, 41]. Although the significance of academic ethics cannot be over-emphasized, however, the present peer-review systems for handling new submissions of academic articles often require manual checking for potential violations of academic ethical rules, which is inefficient for practical uses.

There are still some highly demanded features of paper submission protocols and systems that are missing in existing on-shelf implementations. In particular, in widely-used paper submission systems such as Manuscript Central [18], the submitted but not yet accepted manuscripts are not inherently protected, and malicious reviewers (and in rare cases, the editors) might be able to plagiarize the not-yet-submitted manuscripts as the research results of themselves [9]. In addition, the centralized designs of manuscript submission systems might not be universally trusted by the whole researchers' community, and this problem can be solved by the blockchain technologies [44, 45]. This work is different in that it is based on a purely decentralized blockchain and thus fair for every author, reviewer, and editor.

As a hot technology in the era of digital currencies, blockchain has received lots of research attentions and observed many fundamental technological breakthroughs [2, 7, 8, 19, 27, 28, 31, 47, 48]. To be specific, blockchain exploits a completely distributed ledger [46], which prevents the submitted and accepted manuscripts from being tampered [13, 14, 26, 31, 46], and other people can also verify authenticity of data in the blockchain [45, 48]. Furthermore, the blockchain just stores hash values instead of the data themselves [44, 48], and can be utilized to verify the existence of sensitive data, such as the unaccepted manuscripts. Summarized, the blockchain is an ideal carrier of submitted academic manuscripts for secure plagiarism checking.

The rapid advances of blockchain technologies have driven the emergence of diversified applications. Specifically, because the information saved on blockchain is inherently resistant against malicious tampering, blockchains are suitable for persistently keeping important information for verification purposes, such as electronic graduation diplomas [19], electronic medical records [6], or traceability agricultural products (TAPs) [20].

5. Conclusion and Future Work

The significance of academic ethics has been widely identified, and, with the increasing events of violations of academic ethic rules, the present review system of academic papers urgently needs to be renovated to prevent or detect such violations in an effective way. In this paper, we propose to utilize blockchain technologies to design a paper submission system and accompanying paper submission protocol, so as to guarantee author nonrepudiation and check for explicit plagiarisms. The proposed system and protocol are then verified through analytical studies, where the obtained results are quite encouraging.

As our key future work, we shall incorporate the technologies of *natural language processing (NLP)* and *machine learning (ML)* to more precisely analyze the semantics of academic papers, so as to more effectively detect "implicit" plagiarisms. We shall also seek for the integration of *fully homomorphic encryption (FHE)* in our plagiarism checking strategy, so as to better preserve the secrecy of submitted, but not yet accepted, manuscripts.

Conflicts of Interest

The authors declare no conflict of interest.

References

[1] Zhu, L., Wu, Y., Gai, K., & Choo, K. K. R., "Controllable and trustworthy blockchain-based cloud data management," *Future Generation Computer Systems*, vol. 91, pp. 527–535, 2019.

[2] Yuan, C., Xu, M., Si, X., & Li, B., "Blockchain with accountable CP-ABE: how to effectively protect the electronic documents," IEEE 23rd International Conference on Parallel and Distributed Systems (ICPADS), pp. 800–803, December 2017.

[3] Magrahi, H., Omrane, N., Senot, O., & Jaziri, R., “NFB: A Protocol for Notarizing Files over the Blockchain,” 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS), pp. 1–4, IEEE, February 2018.

[4] Liapidevskiy, A. V., Petrov, A. S., Zhmud, V. A., & Sherubneva, I. G., “Shortcomings of existing systems for registration and legal protection of software products and possible ways to overcome them,” Journal of Physics: Conference Series, vol. 1015, No. 4, p. 042066, IOP Publishing, May 2018.

[5] Jiang, Zhongyun, "Research and Design of Electronic Evidence Preservation Platform based on Block Chain and Merkle Tree," International Conference on Transportation & Logistics, Information & Communication, Smart City (TLICSC), Atlantis Press, 2018.

[6] Irving, Greg, and John Holden, "How blockchain-timestamped protocols could improve the trustworthiness of medical science," F1000Research 5, 2016.

[7] Casino, Fran, Thomas K. Dasaklis, and Constantinos Patsakis, "A systematic literature review of blockchain-based applications: current status, classification and open issues," *Telematics and Informatics*, pp. 55–81, 2018.

[8] Emmadi, Nitesh, Lakshmi Padmaja Maddali, and Sumanta Sarkar, "MaRSChain: Framework for a Fair Manuscript Review System Based on Permissioned Blockchain," *European Conference on Parallel Processing*, Springer, Cham, pp. 355–366, 2018.

[9] OMICS International,” OMICS Peer Review Process,” [Online]. Available: https://www.omicsonline.org/peer-review-process.php, [Accessed Feb. 28, 2019].

[10] Navadiya, K., Contractor, D., Jadhav, M., Mehta, D., & Lakhanotra, R., “Marksheet Validation Using Blockchain,” International Journal of Innovative Knowledge Concepts, 6(Special: 2), pp. 133–136, 2018.

[11] Tenorio-Fornés, Antonio, et al., "Towards a Decentralized Process for Scientific Publication and Peer Review using Blockchain and IPFS," *Proceedings of the 52nd Hawaii International Conference on System Sciences*, 2019.

[12] Spearpoint, M., “A proposed currency system for academic peer review payments using the blockchain technology,” *Publications*, 5.3:19, 2017.

[13] Novotny, Petr, et al., “Permissioned blockchain technologies for academic publishing,” *Information Services & Use*, Preprint, pp. 1–13, 2018.

[14] van Rossum, Joris, "Blockchain for research," *Science*, November 2017.

[15] Ivo Kubjas, “Using blockchain for enabling internet voting,” 2017.

[16] Enago Academy, “8 Most Common Types of Plagiarism to Stay Away from!” Sep, 2018. [Online]. Available: https://www.enago.com/academy/fraud-research-many-types-plagiarism/. [Accessed Mar.4, 2019].

[17] Helen Eassom, “10 Types of Plagiarism in Research,” February 2016. [Online]. Available: https://www.wiley.com/network/researchers/submission-and-navigating-peer-review/10-types-of-plagiarism-in-research. [Accessed Feb. 28, 2019].

[18] IEEE, “Manuscript Central,” [Online]. Available: https://ieee-sensors.org/manuscript-central/ .[Accessed Feb. 28, 2019].

[19] CHEN, Guang, et al., “Exploring blockchain technology and its potential applications for education,” *Smart Learning Environments*, 5.1:1, 2018.

[20] Galvez, Juan F., J. C. Mejuto, and J. Simal-Gandara, "Future challenges on the use of blockchain for food traceability analysis,” TrAC Trends in Analytical Chemistry, vol. 107, pp. 222–232, Oct 2018.

[21] Bodó, Balázs, Daniel Gervais, and João Pedro Quintais, "Blockchain and smart contracts: the missing link in copyright licensing?" *International Journal of Law and Information Technology*, 26.4, pp. 311–336, 2018.

[22] Gattermayer, Josef, and Pavel Tvrdik, "Blockchain-based multi-level scoring system for P2P clusters," *46th International Conference on Parallel Processing Workshops (ICPPW)*, IEEE, pp. 301–308, 2017.

[23] Wang, Maoning, Meijiao Duan, and Jianming Zhu, "Research on the Security Criteria of Hash Functions in the Blockchain," *Proceedings of the 2nd ACM Workshop on Blockchains, Cryptocurrencies, and Contracts*, ACM, pp. 47–55, 2018.

[24] Konashevych, Oleksii, "The concept of the blockchain-based governing: Current issues and general vision," *The Proceedings of 17th European Conference on Digital Government ECDG*, pp. 79, 2017.

[25] Martens, Daniel, and Walid Maalej, "ReviewChain: untampered product reviews on the blockchain," *Proceedings of the 1st International Workshop on Emerging Trends in Software Engineering for Blockchain*, ACM, pp. 40–43, 2018.

[26] Janowicz, Krzysztof, et al., "On the prospects of blockchain and distributed ledger technologies for open science and academic publishing," *Semantic Web* Preprint, 1-11, 2018.

[27] van Rossum, Joris, "The blockchain and its potential for science and academic publishing," *Information Services & Use* Preprint, 1–3, 2018.

[28] Hoffman, Michał R., et al., "Smart papers: Dynamic publications on the blockchain," *European Semantic Web Conference. Springer*, Cham, pp. 304–318, 2018.

[29] De Filippi, Primavera, and Samer Hassan, "Blockchain technology as a regulatory technology: From code is law to law is code," arXiv preprint arXiv:1801.02507, 2018.

[30] An, Jian, et al., "Crowdsensing Quality Control and Grading Evaluation based on a Two-consensus Blockchain." *IEEE Internet of Things Journal*, Nov 2018.

[31] Bai, Yu, et al., "Researchain: Union Blockchain Based Scientific Research Project Management System." *Chinese Automation Congress (CAC)*, IEEE, pp. 4206–4209, 2018.

[32] Gräther, Wolfgang, et al., "Blockchain for education: lifelong learning passport." *Proceedings of 1st ERCIM Blockchain Workshop*, European Society for Socially Embedded Technologies (EUSSET), 2018.

[33] Dima, George-Andrei, et al., "Scholarium: Supporting Identity Claims Through a Permissioned Blockchain," *IEEE 4th International Forum on Research and Technology for Society and Industry (RTSI)*, pp. 1–6, 2018.

[34] Scerbakov, Alexei, Frank Kappe, and Nikolai Scerbakov, "Block-Chain Based Grading Students Assignments," *Proceedings of 11th International Conference of Education, Research and Innovation.* International Academy of Technology, Education and Development, pp. 8773–8778, 2018.

[35] Swist, Teresa, and Liam Magee, "Academic Publishing and its Digital Binds: Beyond the Paywall towards Ethical Executions of Code," *Culture Unbound: Journal of Current Cultural Research*, 9.3, pp. 240 –259, 2018.

[36] Maslove, David M., et al., "Using Blockchain Technology to Manage Clinical Trials Data: A Proof-of-Concept Study," *JMIR medical informatics*, 6.4, 2018.

[37] Gilda, Shlok, and Maanav Mehrotra, "Blockchain for Student Data Privacy and Consent," *International Conference on Computer Communication and Informatics (ICCCI)*, IEEE, pp. 1–5, 2018.

[38] Mthethwa, Sthembile, Nelisiwe Dlamini, and Graham Barbour, "Proposing a Blockchain-based Solution to Verify the Integrity of Hardcopy Documents," *International Conference on Intelligent and Innovative Computing Applications (ICONIC)*, IEEE, pp. 1–5, 2018.

[39] Benet, Juan, "Ipfs-content addressed, versioned, p2p file system," arXiv preprint arXiv:1407.3561, 2014.

[40] Engels, Steve, Vivek Lakshmanan, and Michelle Craig, "Plagiarism detection using feature-based neural networks," *ACM SIGCSE Bulletin*, 39.1, pp. 34–38, 2017.

[41] Laxmi, Muthu Maha, "Research Plagiarism and its Effects," *International Journal of Recent Research Aspects*, pp. 736 –738, 2018.

[42] Caplan, Arthur L, and Barbara K. Redman, "Plagiarism," *Getting to Good*, Springer, Cham, pp. 261–370, 2018.

[43] Smith, Eldon R, "Plagiarism, self-plagiarism and duplicate publication." *The Canadian journal of cardiology*, 23.2, pp.146–147, 2007.

[44] Gipp, Bela, et al., "Cryptsubmit: introducing securely timestamped manuscript submission and peer review feedback using the blockchain," *Proceedings of the 17th ACM/IEEE Joint Conference on Digital Libraries*, IEEE Press, pp. 273–276, 2017.

[45] Jiang, Peng, et al., "Searchain: Blockchain-based private keyword search in decentralized storage," *Future Generation Computer Systems*, Sep 2017.

[46] Abeyratne, Saveen A., and Radmehr P. Monfared, "Blockchain ready manufacturing supply chain using distributed ledger," *International Journal of Research in Engineering and Technology*, 05(09), pp. 1–10, 2016.

[47] Zyskind, Guy, and Oz Nathan, "Decentralizing privacy: Using blockchain to protect personal data," *Security and Privacy Workshops*, IEEE, pp. 180–184, 2015.

[48] Crosby, Michael, et al., "Blockchain technology: Beyond bitcoin," *Applied Innovation*, 2.6-10: 71, 2016.

[49] Ware, Mark. "Online submission and peer-review systems," *Learned publishing*, 18.4, pp. 245–250, 2015.

[50] Ravenscroft, James, Maria Liakata, and Amanda Clare, "Partridge: An effective system for the automatic cassification of the types of academic papers," *International Conference on Innovative Techniques and Applications of Artificial Intelligence*, Springer, Cham, pp. 351–358, 2013.

[51] Liu, Paul Tak Shing, "Medical record system using blockchain, big data and tokenization," *International conference on information and communications security*, Springer, Cham, pp.254–261, 2016.

[52] Sharples, Mike, and John Domingue, "The blockchain and kudos: A distributed system for educational record, reputation and reward," *European Conference on Technology Enhanced Learning*, Springer, Cham, pp. 490–496, 2016.

[53] Ascribe, "ascribe," [Online]. Available: https://www.ascribe.io/. [Accessed Feb. 28, 2019].

[54] Beck, R., Avital, M., Rossi, M., & Thatcher, J. B, "Blockchain technology in business and information systems research," Business & Information Systems Engineering, Vol. 59, Issue 6, pp 381–384, Dec 2017.

[55] Weber, Ingo, et al., "Untrusted business process monitoring and execution using blockchain," *International Conference on Business Process Management*, Springer, Cham, pp. 329-347, Sep 2016.

[56] Aitzhan, Nurzhan Zhumabekuly, and Davor Svetinovic, "Security and privacy in decentralized energy trading through multi-signatures, blockchain and anonymous messaging streams." *IEEE Transactions on Dependable and Secure Computing*, 15.5, pp. 840–852, 2018.

[57] Dreher, Heinz "Automatic conceptual analysis for plagiarism detection." *Journal of Issues in Informing Science and Information Technology*, 4.2007, pp. 601–614, 2007.

[58] Harvey, L. A., et al., "Routine checking of all manuscripts for plagiarism and duplicate publications," Spinal Cord, pp. 427, 2017.

[59] Chowdhury, Hussain A., and Dhruba K. Bhattacharyya, "Plagiarism: taxonomy, tools and detection techniques," *arXiv preprint arXiv*:1801.06323, 2018.

[60] ACM, "ACM Digital Library, " [Online]. Available: https://dl.acm.org/. [Accessed Mar. 8, 2019].

[61] IEEE, "IEEE Xplore Digital Library, " [Online]. Available: https://ieeexplore.ieee.org/Xplore/home.jsp. [Accessed Mar. 8, 2019].

[62] Springer, " Springer, " [Online]. Available: https://www.springer.com/gp. [Accessed Mar. 8, 2019].

[63] ELSEVIER, "ELSEVIER, " [Online]. Available: http://taiwan.elsevier.com/ElsevierDNN/Default.aspx?alias=taiwan.elsevier.com/elsevierdnn/tw. [Accessed Mar. 8, 2019].

[64] Oxford University Press, " Oxford University Press," [Online]. Available: http://global.oup.com/?cc=tw. [Accessed Mar. 8, 2019].

[65] USENIX, " USENIX, " [Online]. Available: https://www.usenix.org/. [Accessed Mar. 8, 2019].

[66] "Open Access Publication & ACM," [Online]. Available: https://www.acm.org/publications/openaccess. [Accessed Mar. 8, 2019].

[67] Bos, Joppe W. et al., "Improved security for a ring-based fully homomorphic encryption scheme," *IMA International Conference on Cryptography and Coding*, Springer, Berlin, Heidelberg, pp. 45–64, Dec 2013.

[68] Armknecht, Frederik, et al., "A Guide to Fully Homomorphic Encryption," *IACR Cryptology ePrint Archive*, 1192, 2015 (2015): 1192.