An Approach for Reviewer Anonymity in Blockchain-Based Peer Review Process

Johann Kandani
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung
Bandung, Indonesia
13521138@mahasiswa.itb.ac.id

Brian Kheng
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung
Bandung, Indonesia
13521049@mahasiswa.itb.ac.id

Michael Utama
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung
Bandung, Indonesia
13521137@mahasiswa.itb.ac.id

***Abstract*—The advancement of blockchain technology has pushed many applications from various domains to adopt the usage of blockchain. The scientific domain is one example which benefits from the use of blockchain, with some focus directed on the publication process. One of the challenges of adopting blockchain technology into the scientific publication process is enabling anonimity in the peer review process. This study approach the use of advancing mixing technology in blockchain to provide *unlinkable* review process, while maintaining the credibility of the reviewer in a blockchain-based peer review process.**

***Index Terms*—Blockchain, Peer review, Privacy, Anonymity, Token mixing**

I. Introduction

Blockchain has revolutionized the technological landscape of digital application for its decentralized nature. This decentralized nature is primarily enabled by its transparency and trustless foundation - by being the trust machine itself [1], [2]. This advancement has been commonly adopted for financial applications, with some of the most popular blockchain platform being Bitcoin and Ethereum [3]. Although most notably known for its use in finance, blockchain has seen some use-cases in other domains [1] including in the scientific world [4].

Current publication process has been subject to improvement primarily in areas regarding the openness of publication result and the credibility of the parties involved in the publication process. This has resulted in some movements we are slowly adopting today such as Open Access [5] that aims to enable free publication results, ORCID [6] that aims to provide credibility and recognition for researchers based on their published works, Open Peer Review [7] which transformed the landscape of peer review process with transparent reviewing process, and more. These efforts however, are still hindered by central authorities and lack of transparency within publication processes. Based on the centralized and transparent nature of the process, blockchain has become a promising tool for publication process for its decentralized nature [4], [8].

Transition to blockchain-based system however, poses new challenges in addition to designing a decentralized organization [9], [10]. One such problem is the peer review process, which is the foundation of most modern publication process [11], [12], [13]. Designing an effective and transparent peer review process on blockchain-based publication system has been the subject of several studies. The proposed designs use smart contracts on the blockchain to provide incentives in the form of tokens [14], [15], [16], [17].

Blockchain inherently provides a degree of anonymity by using public-private key cryptography. This scheme however only provides pseudonymity as transactions can be traced back through blockchain's immutable transaction records. This issue has been subject to studies that aim to increase its privacy and anonymity through cryptography and mixing schemes [18], [19], [20]. The need for privacy and anonymity is also present in the blockchain-based peer review process. A study showed that participants of a blockchain-based publication system highlighted the need for anonymity in peer review process [14]. Anonymity also helps in reducing social bias in reputation-based peer review process [16]. The case for anonymity in peer review process poses different challenges as peer review incentives are linked to the reviewers' identity - which can also be public, verified identity (similar to ORCID [6]) in some cases. This study aims to propose a method that preserves anonymity in general peer review incentive schemes on blockchain-based peer review system.

II. Background

A. Blockchain-Based Peer Review Process

Peer review is a process where experts on the field of the proposed manuscript for publication reviews the work to be published. The review process consists of other reviewers giving their reviews, which is then used as evaluation criteria for the manuscript [12], [13]. There are different schemes for peer review, where some of the well known schemes are summarized in Table I [21], [22]:

TABLE I: Peer Review Schemes

Peer review scheme	Participant knowledge	Identity disclosure
Single blind peer review	Reviewers know the identity of the authors, but the authors do not know the identity of the reviewers	Reviewers identity are not disclosed
Double blind peer review	Neither reviewers nor authors know the identity of each other	Reviewers identity are not disclosed
Open peer review	Both reviewers and authors know the identity of each other	Reviewers identity are disclosed

One of the aim of several blockchain-based peer review process is to enable the transparency of reviews, regardless of whether the reviewers' identity are disclosed or not [4]. These public reviews can then be rated by different participants in the network, either by the participants of the publication process (i.e. authors, editors, and other reviewers) [14], [15], or by separating the concern for verified readers not participating in the publication process of the submitted work [16]. These implementations uses token deployed on smart contracts to reward the reviewers [14], [15], [23].

B. Blockchain Anonymity Schemes

There are levels of privacy that can be achieved in blockchain environment, ranging from pseudonymity, homomorphic encryption, zero-knowledge proofs (ZKP), and K-anonymity. The primary mean to achieve anonymity in blockchain environment is through *unlinkability* [19]. Some of the widely-studied privacy-enhancing methods has been proposed using ZKP, homomorphic encryption, and mixing services [2], [18]. There has been a suggestion for single-use identity approval for accountable anonymous review system, which bases the suggestion with ZKP and mixing service (e.g. Zcash) [24].

Mixing service works by obfuscating the relationship between inputs and outputs [25]. This helps in *unlinkability*, where linking the output to the input will become improbable with higher number of participants [20]. The mixing schemes summarized in Table II [25], [26] provides different ways mixing service can be implemented. Mixing services should also be used with relays to mask the origin of the transaction [27].

TABLE II: Mixing service schemes

Mixing scheme	Scheme
Centralized mixing service	Users provide input to a centrally managed mixing service, which then provides an unlinkable output for the user
Decentralized mixing service	Users provide input to decentralized app on the blockchain which is based on cryptographic technologies such as ZKP
Cross-Blockchain Mixing Service	Users exchanges its input to other blockchain network, then exchanges the output from the other blockchain as the final output back on the origin network

III. Anonymization Scheme

The general scheme used for review voting scheme can be generalized as eligible readers giving their vote (approval or disapproval) of the review given to the reviewer's address (through a smart contract) as depicted in Fig. 1. The plain scheme however, easily links the review given to the reviewer through the transaction. This is not desirable in single blinded or double blinded schemes listed in Table I as the reviewer identities is not to be disclosed.

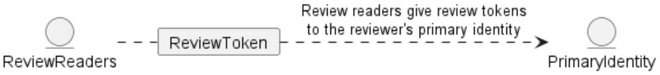
ReviewReaders
ReviewToken
Review readers give review tokens
to the reviewer's primary identity
PrimaryIdentity

Fig. 1: Plain Voting Scheme

To create an *unlinkable* transaction where the votes of the readers contribute to benefit the reviewer's primary identity, a system that cuts the transaction history is needed. For this approach, the use of mixing services are needed. A mixing service obfuscate the trace of transaction from the review to the reviewer. A single-use identity can be used to hold the votes temporarily. However, the usage of single-use identity provides no way for the peer review process to acknowledge that the identity is eligible for reviewing the work.

To ensure that the single-use identity is eligible to give a review, the reviewer can provide access through a "delegation". However, delegating the access will provide a way to link the reviewer to the single-use identity that gives the review. This approach use the same method to *unlink* the delegation through another mixer service. With the new "delegated" identity, the reviewer has the right to give reviews to the current work in review, while keeping the reviewer's identity unlinked to the review. The whole process is summarized in Fig. 2.

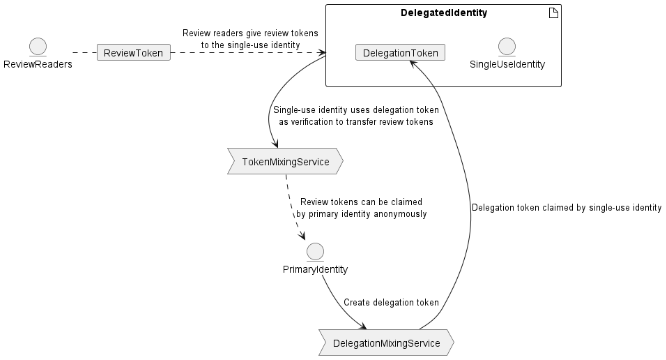
ReviewReaders
ReviewToken
Review readers give review tokens
to the single-use identity
DelegatedIdentity
DelegationToken
SingleUseIdentity
Single-use identity uses delegation token
as verification to transfer review tokens
TokenMixingService
Review tokens can be claimed
by primary identity anonymously
Delegation token claimed by single-use identity
PrimaryIdentity
Create delegation token
DelegationMixingService

Fig. 2: Token Mixing Scheme

IV. Discussion

The proposed solution is only in the form of sketch to protect the privacy of reviewers that provides review in a non-disclosed setting. This study does not explore further on other possibilities that might exhibit vulnerabilities. However, the proposed solution can be used as a starting point or as a sketch for blockchain-based peer review system that requires the reviewers to be anonymous. In some system, where the reviewers are given the right to review with *blind tokens*, the initial mixing approach to obfuscate the single-use identity link can be skipped, and the *blind token* can be directly linked to the single-use identity. This however, does not achieve the same level of anonymity as the granter of the *blind tokens* have the potential to link the reviewer's identity.

V. Conclusion

This study explored the possibility to provide an anonymity setting through the use of *unlinkable* concept based on mixing services. However, the setting for anonymity in the context of peer review requires the reviewer to proof that the reviewer has the required permission to give the review. With further analysis, the same mixing technology can be used to provide a method to "delegate" the permission in the same *unlinkable* way.

References

[1] G. Tripathi, M. A. Ahad, and G. Casalino, "A comprehensive review of blockchain technology: Underlying principles and historical background with future challenges," *Decision Analytics Journal*, vol. 9, p. 100344, Dec. 2023, doi: 10.1016/j.dajour.2023.100344.

[2] F. Casino, T. K. Dasaklis, and C. Patsakis, "A systematic literature review of blockchain-based applications: Current status, classification and open issues," *Telematics and Informatics*, vol. 36, pp. 55–81, Mar. 2019, doi: 10.1016/j.tele.2018.11.006.

[3] S. Corbet, B. Lucey, A. Urquhart, and L. Yarovaya, "Cryptocurrencies as a financial asset: A systematic analysis," *International Review of Financial Analysis*, vol. 62, pp. 182–199, Mar. 2019, doi: 10.1016/j.irfa.2018.09.003.

[4] D. Science and J. van Rossum, "Blockchain for Research," 2017, doi: 10.6084/m9.figshare.5607778.v1.

[5] P. Suber, "What is open access?," *Open Access*, pp. 1–28, Jul. 2012, doi: 10.7551/mitpress/9286.003.0003.

[6] I. Mašić *et al.*, "Sarajevo declaration on integrity and visibility of scholarly publications," *Croatian Medical Journal*, vol. 57, no. 6, pp. 527–529, Dec. 2016, doi: 10.3325/cmj.2016.57.527.

[7] T. Ross-Hellauer, "What is open peer review? A systematic review," *F1000Research*, vol. 6, p. 588, Aug. 2017, doi: 10.12688/f1000research.11369.2.

[8] S. Bartling and B. Fecher, "Blockchain for science and knowledge creation." [Online]. Available: https://doi.org/10.5281/zenodo.60223

[9] C. H. Morales-Alarcón, E. Bodero-Poveda, H. M. Villa-Yánez, and P. A. Buñay-Guisñan, "Blockchain and Its Application in the Peer Review of Scientific Works: A Systematic Review," *Publications*, vol. 12, no. 4, 2024, doi: 10.3390/publications12040040.

[10] S. Leible, S. Schlager, M. Schubotz, and B. Gipp, "A Review on Blockchain Technology and Blockchain Projects Fostering Open Science," *Frontiers in Blockchain*, vol. 2, 2019, doi: 10.3389/fbloc.2019.00016.

[11] D. Banks, "Thoughts on publishing the research article over the centuries," *Publications*, vol. 6, no. 1, p. 10, Mar. 2018, doi: 10.3390/publications6010010.

[12] J. P. Tennant and T. Ross-Hellauer, "The limitations to our understanding of Peer Review," *Research Integrity and Peer Review*, vol. 5, no. 1, Apr. 2020, doi: 10.1186/s41073-020-00092-1.

[13] S. Wessely, "What do we know about peer review?," *Psychological Medicine*, vol. 26, no. 5, pp. 883–886, 1996, doi: 10.1017/S0033291700035224.

[14] Á. Tenorio-Fornés, E. P. Tirador, A. A. Sánchez-Ruiz, and S. Hassan, "Decentralizing science: Towards an interoperable open peer review ecosystem using blockchain," *Information Processing &amp; Management*, vol. 58, no. 6, p. 102724, Nov. 2021, doi: 10.1016/j.ipm.2021.102724.

[15] F. C. Coelho and A. Brandão, "Decentralising scientific publishing: Can the blockchain improve science communication?," *Memórias do Instituto Oswaldo Cruz*, vol. 114, 2019, doi: 10.1590/0074-02760190257.

[16] I. Khan and A. Shahaab, "A peer-to-peer publication model on Blockchain," *Frontiers in Blockchain*, vol. 4, Feb. 2021, doi: 10.3389/fbloc.2021.615726.

[17] Z. Jan, "Recognition and reward system for peer-reviewers," in *ISWC 2018 Doctoral Consortium*, S. Kirrane and L. Kagal, Eds., CEUR-WS.org, Oct. 2018, pp. 46–54. [Online]. Available: https://api.semanticscholar.org/CorpusID:53067073

[18] Y. Yang, K. Jin, W. Liang, Y. Liu, Y. Li, and O. Hosam, "A Review of Blockchain-based Privacy Computing Research," in *2023 IEEE 10th International Conference on Cyber Security and Cloud Computing (CSCloud)/2023 IEEE 9th International Conference on Edge Computing and Scalable Cloud (EdgeCom)*, 2023, pp. 241–246. doi: 10.1109/CSCloud-EdgeCom58631.2023.00049.

[19] F. J. de Haro-Olmo, Á. J. Varela-Vaca, and J. A. Álvarez-Bermejo, "Blockchain from the Perspective of Privacy and Anonymisation: A Systematic Literature Review," *Sensors*, vol. 20, no. 24, 2020, doi: 10.3390/s20247171.

[20] N. Glaeser, M. Maffei, G. Malavolta, P. Moreno-Sanchez, E. Tairi, and S. A. K. Thyagarajan, "Foundations of Coin Mixing Services," in *Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security*, Los Angeles CA USA: ACM, Nov. 2022, pp. 1259–1273. doi: 10.1145/3548606.3560637.

[21] P. A. Ali and R. Watson, "Peer Review and the publication process," *Nursing Open*, vol. 3, no. 4, pp. 193–202, Mar. 2016, doi: 10.1002/nop2.51.

[22] O. Zimba and A. Y. Gasparyan, "Peer review guidance: a primer for researchers," *Rheumatology*, vol. 59, no. 1, pp. 3–8, 2021, doi: 10.5114/reum.2021.102709.

[23] T. K. Mackey, N. Shah, K. Miyachi, J. Short, and K. Clauson, "A Framework Proposal for Blockchain-Based Scientific Publishing Using Shared Governance," *Frontiers in Blockchain*, vol. 2, 2019, doi: 10.3389/fbloc.2019.00019.

[24] A. Tenorio-Fornés, V. Jacynycz, D. Llop-Vila, A. Sánchez-Ruiz, and S. Hassan, "Towards a decentralized process for scientific publication and peer review using blockchain and ipfs," *Proceedings of the Annual Hawaii International Conference on System Sciences*, 2019, doi: 10.24251/hicss.2019.560.

[25] L. Wu *et al.*, "Towards Understanding and Demystifying Bitcoin Mixing Services," in *Proceedings of the Web Conference 2021*, Ljubljana Slovenia: ACM, Apr. 2021, pp. 33–44. doi: 10.1145/3442381.3449880.

[26] R. Xiao, W. Ren, T. Zhu, and K.-K. R. Choo, "A Mixing Scheme Using a Decentralized Signature Protocol for Privacy Protection in Bitcoin Blockchain," *IEEE Transactions on Dependable and Secure Computing*, p. 1, 2019, doi: 10.1109/TDSC.2019.2938953.

[27] M. Moser and R. Bohme, "Anonymous Alone? Measuring Bitcoin's Second-Generation Anonymization Techniques," in *2017 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, Paris: IEEE, Apr. 2017, pp. 32–41. doi: 10.1109/EuroSPW.2017.48.