Towards a Decentralized Process for Scientific Publication and Peer Review using Blockchain and IPFS

Antonio Tenorio-Fornés
GRASIA, Universidad Complutense de Madrid
antoniotenorio@ucm.es

Viktor Jacynycz
GRASIA, Universidad Complutense de Madrid
vsjacynycz@ucm.es

David Llop
GRASIA, Universidad Complutense de Madrid
dallop@ucm.es

Antonio A. Sánchez-Ruiz
GAIA, Universidad Complutense de Madrid
antsanch@ucm.es

Samer Hassan
GRASIA, Universidad Complutense de Madrid
Berkman Klein Center at Harvard University
shassan@cyber.harvard.edu

Abstract

The current processes of scientific publication and peer review raise concerns around fairness, quality, performance, cost, and accuracy. The Open Access movement has been unable to fulfill all its promises, and a few middlemen publishers can still impose policies and concentrate profits. This paper, using emerging distributed technologies such as Blockchain and IPFS, proposes a decentralized publication system for open science. The proposed system would provide (1) a distributed reviewer reputation system, (2) an Open Access by-design infrastructure, and (3) transparent governance processes. A survey is used to evaluate the problems, proposed solutions and possible adoption resistances, while a working prototype serves as a proof-of-concept. Additionally, the paper discusses the implementation, in a distributed context, of different privacy settings for both open peer review and reputation systems, introducing a novel approach supporting both anonymous and accountable reviews. The paper concludes reviewing the open challenges of this ambitious proposal.

1. Introduction

Science publication and peer review are based on a paper-based paradigm that has not seen large changes in the last centuries [1]. Critics to current science publication and peer review systems include concerns about fairness [2], quality [3], performance [4], cost [5], and accuracy of the evaluation processes [6].

The development of the Internet enabled an expansion of the proposals for alternatives for both science dissemination [7] and evaluation [8]. The reduction of distribution costs enabled wider access to scientific knowledge, and questioned the role of traditional publishers [9].

It is acknowledged that the Open Access and Open Science movements have successfully reduced the economic cost of readers to access knowledge [10]. However it has not successfully challenged traditional publishers' business models [11] that are often charging both readers and authors [12].

Traditional peer review has suffered multiple criticisms, and yet only few alternatives have gathered success [13]. The literature provides multiple proposals around open peer review [14], and proposals of reputation networks for reviewers [15]. In fact, a start-up, Publons[1], provides a platform to acknowledge reviews and open them up.

In addition, other alternatives to the traditional science publication process have arisen in the last 20 years. *Preprints* are scientific papers that have not been peer-reviewed, therefore have not been published in a journal or conference. Platforms such as arXiv[2] and Preprints.org[3] have been successful within the scientific community, allowing these pre-published papers to gain more visibility [16].

Social networks have also carved a niche in the community. Platforms such as Academia[4] or Research Gate[5] are being used by more people every day, allowing researchers to upload their published papers, further connecting the scientific community.

Nevertheless, the mentioned platforms are centralized, with an infrastructure typically controlled by a sole private entity. This centralization has multiple implications [17, 18], for example, less control and self-management for the scientific community; a requirement of blind trust in a third-party that can change its terms or policies at anytime (e.g. in case of a buy-in); or problems related to for-profit business

[1]https://publons.com/
[2]https://arxiv.org/
[3]https://www.preprints.org/
[4]https://www.academia.edu/
[5]http://researchgate.com/

URI: https://hdl.handle.net/10125/59901
ISBN: 978-0-9981331-2-6

models which may affect users, or their data.

Decentralized alternatives, despite their promises [19], are still in their infancy. A few proposals, none of them functional to date, have appeared recently: a peer review proposal using cryptocurrencies [20], a blockchain-enabled app with voting and storage of publications, again using cryptocurrencies [21], or a peer review quality control through blockchain-based cohort trainings [22]. Additionally, the new Ledger[6] journal records the publication timestamps in the Bitcoin blockchain.

This paper proposes the development of a decentralized publication system for open science. It aims to challenge the technical infrastructure that supports the middleman role of the oligopoly of traditional publishers [11]. Due to the successes of the Open Access movement, some scientific knowledge is freely provided by publishers. However, the content is still mostly served from their infrastructure (i.e. servers, web platforms). This ownership of the infrastructure gives them power over the scientific community which produces the contents [23]. Such a central and oligopolistic position in science dissemination allows them to impose policies (e.g. copyright ownership, Open Access prices, embargo periods, dissemination restrictions) and concentrate profits.

The proposed system presents the ambitious aim to move the infrastructure control from the publishers to the scientific community. It entails the decentralization of three essential functions of science dissemination: 1) the selection and recognition of peer reviewers, proposing a peer reviewer reputation system where review reports can be rated 2) the distribution of scientific knowledge, through the distribution of scientific papers using the IPFS P2P network, providing an Open Access by-design infrastructure, and 3) peer review process communication, relying on Blockchain to provide a transparent and decentralized platform for open peer review process communications, such as paper submissions, reviewer proposals or review submissions. It specifically targets four issues of the peer review process: 1) the quality, and 2) fairness of peer review from authors' perspectives, 3) the fairness of recognition, reputation or rewards received for reviewing from reviewers' perspectives, and 4) the difficulty in finding good reviewers from editors' perspectives. Additionally, it proposes a decentralized solution aiming to reduce the control of publishers through their centralized infrastructure.

First, Section 2 offers a review of the state of decentralization technologies and introduces the concepts and technologies used in the paper. Then, Section 3 provides an overview of the system's requirements, with a design explained in Section 4 and an implemented prototype described in Section 5. In order to perform a preliminary evaluation of the detected problems and proposed solutions, we have performed a survey described in Section 6, including a discussion of its results. In addition, since the proposed open system raises multiple concerns around privacy, Section 7.1 discusses the opportunities and challenges around different privacy settings regarding peer review in an open and decentralized network. Furthermore, this section introduces a novel approach which enables both anonymous and accountable reviews, bringing together the promises of both blinded [24] and open review [14] models, addressing the concerns about the negative consequences for reviewers of a reputation system. Finally, Section 8 discusses the benefits, challenges, opportunities and open questions arising from the described proposal.

[6] https://ledgerjournal.org

2. Decentralization Technology

As further explored in Section 3, this paper proposes to use decentralized technologies to provide 1) a reputation system for reviewers, 2) an Open Access by-design infrastructure for paper distribution and 3) transparency for peer review governance. This section introduces the decentralization technologies on which the paper proposals to rely. Note the section follows the approach of Tenorio-Fornés et al. [25] which proposes a framework for distributed systems in which IPFS is used for distributing content and Blockchain to provide consistent behavior.

IPFS: IPFS is a decentralized file system which enables the distribution of content in a decentralized network of peers (such as some P2P sharing systems [26]). It also supports secure links among such contents (Merkle-links [27]), enabling the use of complex data structures such as those used in git [28] or blockchain. This paper proposes the use of IPFS to distribute the papers and reviews of the system (see Section 3.2). Thus, papers and reviews can be unambiguously identified in the network by the hash of their data.

Blockchain: Blockchain was the first technology that enabled a fully distributed digital currency, Bitcoin [29]. It solved the double-spending problem by which a dishonest actor may try to spend the same coin twice in decentralized currency systems. It relies on a ledger of transactions that is updated and maintained by a network of peers. The blockchain introduces incentives to maintain the security of the ledger, both rewarding nodes that contribute computational power for the security of the network, and requiring at least half of the computing power of the network to alter the state of the blockchain — i.e. the blockchain is secure if at least half of the computing power is provided by honest peers. This technology enabled a new wave of decentralization of applications such as domain name registries [30] or microblogging platforms[7] . A second wave of blockchain-based decentralization was started by Ethereum [31], as described below.

Ethereum and smart contracts: Ethereum is a blockchain-based distributed computing platform. It started the aforementioned second wave of decentralization [31], which enabled the deployment, on the blockchain, of small code snippets named *smart contracts* [32]. In this technology, the peers of the network execute the code of smart contracts. Similarly to Bitcoin, where a network of peers ensure the validity of a ledger of transactions, in Ethereum a network of peers ensures the execution of these smart contracts. Thus, a smart contract code will be executed as long as there are peers in the network, i.e. it cannot be stopped and it is autonomous from its creators. Also, its rules will be executed as defined by its code, i.e. its rules are self-enforced [33]. Each interaction with Ethereum is registered as a cryptographically signed *transaction*, similarly to Bitcoin. Examples of decentralized applications enabled by this technology include prediction markets [34], social networks [35] or a game to collect, breed, and sell virtual kitties[8]. This paper proposes the use of smart contracts to 1) implement a reviewer reputation system and 2) to enforce the transparency of the peer review rules, for example, who may assign reviewers, or who can submit a review (See Section 4).

3. Requirements

The proposed system aims to provide a distributed platform for open science, from submission to publication, including the peer review process communications. The system rests on three main pillars: a distributed reviewer reputation system, Open Access by-design, and transparent governance. These are outlined in the following subsections.

3.1. A Distributed Reviewer Reputation System

The information concerning the quality and reliability of reviewers is usually private to publishers and journals (and even editors). There is no easy way to predict the quality of a reviewer from factors such as training and experience [36]. Although this information is valuable, it is kept private, reinforcing the publishers' and journals' influential positions.

This proposal extends traditional peer review communication workflow with the possibility of rating peer reviews, building a reputation system for reviewers [37]. Reviewers are rewarded for worthy, fair, and timely reviews, or penalized otherwise.

This open reputation network of reviewers could increase the visibility and recognition of the reviewers [38]. In fact, such incentives could even be monetary, using cryptocurrencies [39]. In addition, creating a public reputation network for reviewers reduces, or at least exposes, unfair and biased reviews [2, 40].

3.2. Open Access By-Design

Open Access focuses on free access to scientific knowledge. While publishers provide Open Access content free of charge, their control of the science dissemination infrastructure allows them to impose certain rules, such as charging authors unreasonable fees to offer their work as Open Access (Gold Open Access) [41] or the temporary embargo and restrictions on the dissemination of the final version (Green Open access) [42], among others.

Our system proposes a decentralized infrastructure for science publications. Academic documents - from first drafts to final versions, including peer reviews - are shared through IPFS, an open P2P network [43] described in the previous section. In this type of P2P networks, it is substantially difficult to impose restrictions on content access and sharing. Thus, the system inherently (by-design) facilitates Open Access through its distributed infrastructure, circumventing publishers' dominant roles. Moreover, the access to these documents does not depend on the existence of our platform. Even if our platform ceases to exist, the documents could still be retrieved from the network.

3.3. Transparent Governance

Nowadays, the peer review process is digitally supported, yet some argue that the system remains feudal [9]. There are multiple proposals to improve peer reviews [8], yet communications and processes remain closed and under the control of journals and publishers, and thus depend on their specific infrastructures [40].

The proposed system aims to improve the transparency, speed and fairness of the peer review process. In order to do this, the system proposes to support the peer review interactions in an open and decentralized network. It registers, in a public

[7] http://twister.net.co/
[8] https://www.cryptokitties.co/

decentralized ledger, the following parts of the publication process: paper submission, assigning reviewers, review submission and paper publication. Thus, processes like the selection of reviewers, or the contents of the reviews, are open to the public. With interactions being time-stamped and tamper-proof thanks to blockchain technology, they can be monitored, audited, and held accountable. More complex iterations of the system may consider blind reviews (Section 7.1).

Opening the peer review process communications to the public could even change the acceptance dynamics within the system. Currently, high rejection rates are encouraged because the risk of rejecting a relevant paper is negligible, while the acceptance of less relevant content is penalized [9, 44]. However, within a more transparent system, the first may be penalized as well.

This transparency, combined with a distributed infrastructure for peer review, facilitates the exploration of new workflows [40].

4. Design using a Decentralized Infrastructure

The system provides a platform for the peer review process communications, from paper submission to paper acceptance or rejection, and supports the rating of peer reviews to build a reviewer reputation network.

The proposed system relies on the technologies mentioned in section 2. On one hand, the *Ethereum blockchain* provides a public decentralized ledger to record the system's interactions. Smart contracts are used to enforce the rules of the system, such as only accepting reviews of invited reviewers. On the other hand, *IPFS* provides a distributed file system to store the content of the peer review process. This ensures that the information registered in the platform will be persistent, free and accessible, and will not rely on a centralized server.

The sequence diagram of the system (Figure 1) describes the main interactions of supported peer review governance. Below we proceed to describe these interactions and the basic ideas to implement them.

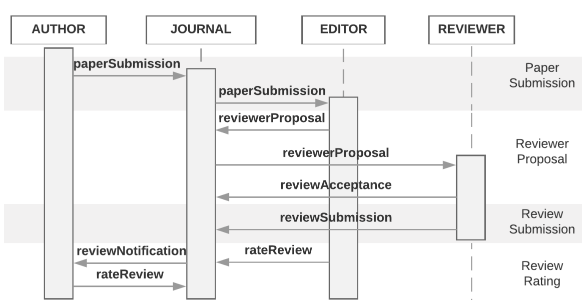

Figure 1. Sequence diagram of platform interaction

Paper submission: The submission process has three steps within the system. First, the paper is uploaded to the IPFS network, then the platform will recover the unique identifier of that paper, the IPFS address. Finally, the platform will create an Ethereum *smart contract* containing the file address and the addresses of the authors to record the submission on the blockchain. This creates a transaction in Ethereum that can be used to verify that the authors submitted the paper. Furthermore, this *smart contract* generates an Ethereum address that acts as a paper's unique identifier inside and outside the platform.

Reviewer proposal: A journal editor may invite a reviewer to review a specific paper, creating a *review task* in the paper's *smart contract*. The transaction will record the Ethereum address of the reviewer and, optionally, a deadline to submit the review. The invited reviewer may accept or reject the *review task* (which will also be recorded into the blockchain). If the task is rejected, the editor can assign another reviewer.

Submit review To submit a review, the reviewer should carry out a transaction that will record the acceptance/rejection and the IPFS address (i.e. the location) of the detailed review. In the event of a reviewer sending a review when the time has expired, a penalty is applied to the reviewer's reputation in the reputation system.

Rate review A novelty of the system discussed in Section 3.1 is the reputation system for reviews. A blockchain transaction will record the sender address and the rating as well as the rated review and reviewer addresses.

5. Implementation

In order to implement the system, we developed a proof-of-concept prototype that allowed us to perform preliminary testing of each interaction within the platform, exploring the feasibility of its implementation using the aforementioned decentralized technologies. Thus, this software implements a basic version of the requirements specified in Section 3, and follows the design of Section 4. The software is free/open source, available in Github[9].

The architecture relies on 1) IPFS for distributed storage of papers and review reports and 2) Ethereum Blockchain for the system's logic and state. The prototype proposes an HTML + JavaScript interface that connects to IPFS and Ethereum through JavaScript clients and uses Metamask[10] to provide an user-friendly management of Ethereum user identities.

[9] https://github.com/DecentralizedScience/Gateway
[10] https://metamask.io

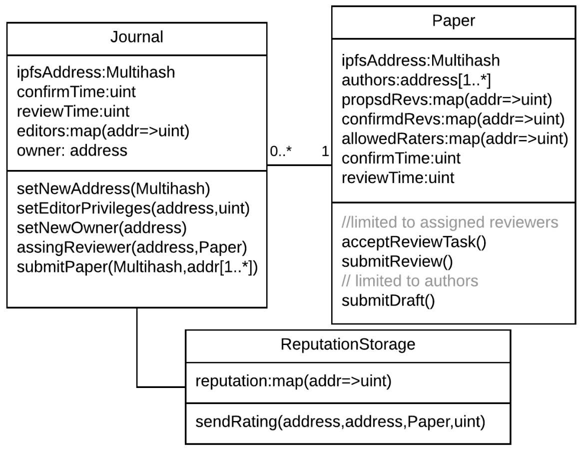

Figure 2. Smart contract diagram of the platform

This proof-of-concept prototype uses three different Ethereum smart contacts to run the platform's inner functioning. Figure 2 shows a diagram of this structure. The *Multihash* structure is used to store IPFS references in the system. The *Journal* contract controls the paper submission, the selection of editors, the assignment of reviewers, and the acceptance of reviewers. The *Paper* contract identifies a paper within the system, controls the review submissions, and shares who may rate a review. Finally, the *ReputationStorage* contract stores the ratings of the peer reviews, receive new rates, updating the reputation of reviewers if allowed by their Paper contract, and shares the reviewers' reputation.

6. Evaluation

A Likert scale survey [45] was conducted to assess (1) the importance for respondents of the tackled peer review process problems, (2) to which degree they believe a reviewer reputation system may help to improve them and (3) to which extent they would experience some resistance towards the solution. The survey constitutes an exploratory study of the validity of the proposed solution. It addresses academic researchers interested in the problems of peer review processes. Its design follows a convenience non-probability sampling: three different groups of academics that may be interested in the solution took part in the survey; namely 1) a Telegram group of 166 members ("Open Science Ecosystem") for projects building decentralized solutions for open science, 2) the Computer Science department the authors are members of, and 3) a list of 36 people who have subscribed to a newsletter available on our prototype website. Thus, the survey does not aim to generalize the results for the whole academic researcher population; its purpose is to explore the response of potentially interested users of different profiles. That is, would this proposal attract enough early adopters which would enable further exploration and validation? The survey is solely targeted for academic researchers, although the questions are intended to be answered from the perspective of three different roles: as authors, reviewers or editors.

The survey first collects data for the characterization of the population: age, gender, whether the respondent is (or has been) an academic, and current participation in research groups or open science projects.

Afterwards, the survey questions the perception of the importance of the peer review problems, the possible resistance to a reviewer reputation system, and the perceived adequacy of such a system to solve the explored problems. These perceptions are investigated using a 1 to 5 Likert scale to measure agreement with the statements, where 1 means 'strongly disagree' and 5 'strongly agree'.

Problem questions: The survey asked the following questions related to the problems of the review process: 1) As an author, I think that the quality of the review process can be sensibly improved. 2) As an author, I think that the fairness of the review process can be sensibly improved. 3) The recognition, reputation or rewards I receive as a reviewer feels fair in relation to the amount of work that I do. 4) As an editor, I have difficulties finding good reviewers (quality, relevance, timeliness).

Resistance responses: Afterwards, the survey enquires about the following possible resistance for the adoption of a reviewer reputation system: 5) As an author, I would prefer to submit my work to a journal in which reviews can be publicly rated (on a reviewer reputation system), 6) As a reviewer, I would prefer to submit a review to a journal in which my review would be publicly rated (on a reviewer reputation system), 7) As a reviewer, I would only submit a review to a journal which rates its reviews, if I remain anonymous. 9) As an author/editor/reviewer, I would like to be able to rate the reviews of the papers I am working with.

Problem/solution fit responses: Finally, the survey asks, for each of the four explored problems, if the respondents believe that a reputation system of reviewers may sensibly contribute to address them. 8) As an editor, I would find a reviewer system sensibly useful to find relevant, timely and/or high quality reviewers. 10) I believe that a reviewer reputation system could sensibly improve the quality and/or fairness of the peer review process. 11) I believe that a reviewer reputation system could sensibly improve the recognition, reputation or rewards I receive for my reviews.

Question	#Answers	mean*	mode
1) quality	35	4.2	4
2) fairness	36	4.4	5
3) rev. fairness**	34	2.4	2
4) finding reviewers	30	3.9	3 or 4
5) author resistance	36	3.9	4
6) reviewer resistance	34	3.6	4
7) anon. rev. resistance	34	3.1	3
8) improve rev. search	30	3.9	4
9) want to rate	36	4.3	5
10) improve qual./fair.	36	4.1	4
11) improve recog.	35	3.9	4

*Max of 5. **Perceived fairness, i.e. lower the better

Table 1. Summary of Likert scale 1 to 5 responses

6.1. Results

The survey was responded to by 37 people, of which one was filtered out as a non-researcher. The results of the survey are summarized below.

33 of the participants are academic researchers, while 3 have been academic researchers in the past. 8 responded that they do not participate in a research group or a project related to open science or did not responded to that question. The age ranges 18-24, 25-34, 35-44 and 45+ are distributed as 1, 11, 14 and 10 participants respectively. 10 are female and 26 male (none chose other or not responded).

The responses to the 11 likert scale questions with the 1 to 5 scale are summarized in Table 1.

6.2. Results discussion

The four explored problems seem to be relevant for the participants. Note that question 3 is inversed with respect to the other questions, as it asks for the perceived fairness of the current process (and not unfairness). Questions 1 and 2 present the strongest results, as their means are between agreement and strong agreement. Questions 3 and 4 have an average between (dis)agreement and neutral, thus, the perceived relevance of these problems is relatively smaller than the former.

The three questions assessing possible resistances for the adoption of the solution show that both authors and reviewers would prefer to use the proposed solution. In fact, only 4 participants disagree in their preference of the proposed system in each question. With regards to anonymity, 14 reviewers agree or strongly agree that anonymity is a needed condition for their participation in the system, while most respondents remain neutral or disagree with this need. Participants agree that they would like to rate reviews (average between agree and strongly agree).

Finally, the use of a reputation system for reviewers is perceived as a relevant solution for the explored problems with averages close to agreement: 3.9 for finding reviewers, 4.1 for improving quality or fairness and 3.9 for recognition and reputation of peer reviewers.

Overall, it is considered that this small survey provides a preliminary evaluation which invites further exploration of the proposed solution. It is also an indication that such a system could attract early adopters with whom to perform further testing.

7. Privacy requirements

Given the concerns around privacy in the proposed system, and following the feedback received, we have explored an extension of this system, taking into account different privacy settings and their potential implementations.

In traditional peer review, there are several privacy settings that can be adopted, allegedly to improve the fairness of the process [24, 46]: (1) Blind reviews, which keeps reviewers anonymous, protecting their freedom to criticize. (2) Double blind reviews, which keeps both authors and reviewers anonymous, to prevent social bias. (3) Open reviews, in which both authors and reviewers are known, with effects under debate [47, 48]

7.1. Privacy requirements for Reviewer Reputation Systems

	Public Reviewer	**Anon. Reviewer**
Public Rater	Signed rate of open review	Signed rate of blind review
Anon. Rater	Anonymous rate of open review	Anonymous rate of blind review

Table 2. Different configurations to rate a review

This section builds on the described traditional privacy settings, adding a new layer of complexity: we not only deal with reviews, but with both reviews and ratings. As already proposed in Section 3.1, the construction of a reputation network of reviewers may improve the accountability of the peer review process. Thus, this section explores different privacy settings such reputation systems may have. One of these settings, the rating of blind reviews, is explored in more detail. Challenges of such systems are identified, and will later guide the discussion in subsection 7.2 on how this may be achieved.

Signed Rating. Similarly to the open peer review (explained above), signed ratings are both public and verified ratings of a review. It is straightforward to implement by maintaining a public identity for the raters.

Anonymous Rating. Protecting the identity of raters is interesting in several reputation systems [49]. We can support this anonymity feature using *blinded tokens* [49] that grant permission to rate without revealing the identity of the rater. People authorized to rate a review in the system, e.g. authors, editors and other reviewers of the paper involved in the process, may each get one of these tokens.

Rating Blind Reviews. The question of whether we can keep the benefits of blind reviews while providing accountability and recognition to reviewers (and thus rating their reviews) deserves special consideration, and thus it is explored below.

The following challenges must be considered in order to provide the Rating Blind Reviews privacy setting:

Challenge 1 (Anonymity) *The reviewer should be able to claim the rating received in her review (e.g. to receive a positive reputation) without revealing that she is the author of the review.*

Challenge 2 (Accountability) *The reviewer should not be able to avoid the effect of negative reviews (e.g. only claiming the positive ratings).*

Challenge 3 (Authorization) *The ratings should come from authorized raters (i.e. minimizing cheating).*

Challenge 4 (Sybil resistance) *Having several identities in the system should not provide advantages. Note that blockchain systems such as Ethereum allow the creation of multiple identities per user.*

Challenge 5 (System abuses) *The anonymity of interactions may hinder the detection and prevention of system abuses. For instance, malicious actors may try to submit fake reviews to be rated by accounts they control in order to obtain unfair good ratings. Detecting this behavior would not be trivial since reviews and ratings may be anonymous.*

A system allowing an anonymous yet accountable reputation system for peer reviewing would enable a new privacy and accountability model for peer reviews. However, its implementation faces important challenges such as those described above. The next section provides an overview of how existing techniques may be applied to tackle the identified challenges.

7.2. Achieving Accountable Anonymous Reviews

The previous section identifies challenges that an anonymous yet accountable reputation system for peer reviews faces. Some existing technologies have been applied to similar challenges, and others may help to combine their advantages. This section explains these technologies and how they may be used to tackle the challenges of this system. First it provides an overview of how the technologies may be combined, and a description of the technologies follows.

A simple way of protecting the identity of users is the use of different virtual identities for each interaction, i.e. *single-use identities*. However, linking the reputation received by these single-use identities to their real identity, both providing accountability (Chlg. 2) and preserving anonymity (Chlg.1), requires the use of other technologies.

In order to provide accountability (Chlg. 2), the system may try to detect when an identity has not received a bad reputation. For this purpose, a reputation deposit or *collateral* could be requested for each rating a reviewer may receive. This way, users could compare the number of claimed ratings and the number of unclaimed ratings, and assume bad ratings for those that are missing. This collateral-based technique should be applied carefully, avoiding abuses such as trying to use the same collateral for different ratings. Advanced cryptographic techniques such as *zk-SNARKs* (explained below) may help to prove that these requirements are met without compromising a reviewer's identity. These techniques may be used to allow a reviewer to claim a rating from a review she carried out without revealing her identity but proving her authorship (Chlg. 1).

A different issue is to allow ratings to come solely from authorized raters (Chlg. 3). To fulfil these authorization requirements, several techniques such as *blind signatures* or *blind tokens* may be used. These would enable permission to be granted to a collection of identities to perform an action, e.g. rate a review, without revealing which of them voted, or which voted for what. As previously mentioned, *single-use identities* may be used to provide anonymity; in this case, for raters.

Allowing only authorized rates, as previously explained, may help to prevent Sybil attacks (Chlg. 4). Moreover, the cost of losing a reputable identity may reduce the attractiveness of creating a new identity simply to gain a reputation.

The use of the mentioned zk-SNARKs may also help to prevent some system abuses. For instance by enabling the use of cryptographic proofs that verify that the ratings come from reviews submitted to reputable journals, would prevent fake reviews and ratings.

Next, the mentioned technologies are explained.

Single-use identities: New single-use identities may be used as a simple technique to support anonymous interactions (Chlg. 1). However, supporting the authorization rules of the system (Chlg. 3) and providing accountability (Chlg. 2) for those identities are challenges that require consideration.

Ring signatures: Ring signatures [50] are a cryptographic technique that allows the authorization of a collection of identities to perform an action, while maintaining the privacy of the specific identity that performed the action. They may be used to authorize rates to a group of identities without revealing who rated what or who rated. Thus, this technique may be used to support the authorization requirements of the system (Chlg. 3), while providing some anonymity to the users (Chlg. 1). Note that with this technique, the identities of those who may have signed are known, so the combination with other anonymity measures could be of interest.

Blind tokens: In the context of an election and using a cryptographic technique called blind signatures [51], it is possible to create ballots for authorized actors that preserve the anonymity of the vote (both hiding who casted a vote and what each actor voted) but ensuring that only authorized voters participated. Note that, as with ring signatures, the identities of those who may have signed are known, and thus complementary anonymity measures could be used. This technique has been also used to anonymize a distributed reputation system [49]. Thus, it could be used to provide anonymity to reviewers and raters (Chlg. 1) while supporting the authorization rules of the system (Chlg. 3).

Collateral pattern: In order to secure the funds needed for a blockchain application to function, it is common that the application requires the participants to pay for the assets they may lose as collateral. For instance, a betting smart contract will first ask all participants to pay their bets and afterwards distribute the prices. This paper calls this technique ”collateral pattern”, and proposes its use to provide accountability (Chlg. 2) to the reviewers of the reputation system (Section 3.1). For each rating a reviewer may obtain, the reviewer must spend as much reputation as she may lose. This encourages the claiming of bad ratings, since not claiming them may result in a bigger loss.

zk-SNARK: is a cryptographic procedure enabling a statement to be proved without revealing anything else; that is, apart from the evaluation if the statement is in fact true (zero-knowledge proof of knowledge) [52] . The same authors also provide this property in a succinct and non-interactive fashion, for example, using a relatively small proof and not requiring further communication between prover and verifier. In fact, the popular Zcash project uses this technology to build an anonymous cryptocurrency [53]. Proving statements in this privacy preserving manner is of great interest for several challenges of the proposed accountable anonymous review system. For instance, proving that a user controls a single-use identity may allow the user to claim the reputation given to that identity (Chlg. 1). Additionally, a reviewer may prove that she paid the reputation collateral needed to submit a review without revealing her identity and without being able to use the same collateral for another review (Chlg. 2). Finally, proving that the reputation comes from a review submitted to a collection of honest journals that do not allow abuses, may help to mitigate the abuses that fake reviews and ratings represent for the system (Chlg. 5).

8. Discussion and Concluding Remarks

This paper proposes the opening and decentralization of three of the peer review and publication functions: 1) the selection and recognition of peer reviewers, 2) the distribution of scientific knowledge, and 3) the peer review process communication. Arguably, this decentralization of the infrastructure could help to challenge the central role of middlemen such as traditional publishers.

Distributed technologies such as blockchain and IPFS may finally realize the promise of Open Access, while enabling new models of science dissemination. Opening and decentralizing the infrastructure enhances the transparency and accountability of the system, and may provide a new arena to foster innovation. Note that the proposed system does not rely on the use of cryptocurrencies, since it is focused on a not-for-profit approach, far from the startup-driven commercial approaches common in the blockchain space.

The transparency provided by opening the peer review process allows the construction of a reputation system of reviewers, but also raises concerns about privacy and fairness. Furthermore, the introduction of a new public metric (reviewers' reputation) may also affect researcher careers, adding pressure to the already straining processes for academic survival [54]. A working prototype was developed as a proof-of-concept of the reviewer reputation system proposal. This work uses a survey to evaluate the perceived importance of four peer review process problems and if a reviewer reputation system is perceived as a solution for them, as well as the possible resistance to adoption that the proposal may suffer. The results suggest that the four problems are relevant, especially peer review quality and peer review fairness. The studied resistance to adoption seems low while the participants agree they would like to use the proposal. Additionally, the participants seem to agree that the solution addresses the studied problem.

Still, some challenges of the system remain open as future work, such as the detection and prevention of fake science, journals, and conferences or the detection and prevention of fake reviews, or revenge ratings to game the reputation system.

Blockchain technologies can be used to replicate the privacy settings currently used in peer review processes. However, Blockchain can also be used to introduce a new review model that supports the accountability of peer reviewing while maintaining the anonymity of blind and double blind reviews to improve fairness. The implications of such accountable, open and anonymous review models are still to be revealed, since an incentive based reputation system it could also support negative dynamic changes such as increasing competitive dynamics, or gender bias.

Additionally, the proposed system's infrastructure relies on new technologies with their own challenges. Blockchain technologies face scalability issues, transaction costs, inclusiveness and usability problems that remain open and under discussion. On the other hand, distributed file systems such as IPFS may be more resilient, but they still need somebody in charge of preserving and providing data, since without that responsible actor, it may result in an unpredictable loss of content. Considering these archiving issues, whether this new technologies will allow the creation of durable science repositories able to interoperate with legacy, current and future systems remain open.

Other open issues that require further research and may be explored in future work are the implementation of the proposed privacy settings, the exploration of different copyright regimes, the challenging of traditional journal-centered metrics to rate publication quality, different reputation algorithms, different levels of openness, and the exploration of decentralized autonomous journals.

Despite the existing challenges, we are confident that decentralizing the processes that Science relies on, would open up a whole new playing field, with implications we cannot possibly foresee. Will its benefits outweigh its risks? We believe it is a conversation worth having.

Acknowledgments

This work was partially supported by the project P2P Models (`https://p2pmodels.eu`) funded by the European Research Council ERC-2017-STG (grant no.: 759207), and the Spanish Ministry of Economy, Industry and Competitiveness (TIN2014-55006-R, TIN2017-87330-R) and the UCM (Group 921330).

References

[1] R. Spier, "The history of the peer-review process," *TRENDS in Biotechnology*, vol. 20, no. 8, pp. 357–358, 2002.

[2] C. Wenneras and A. Wold, "Nepotism and sexism in peer-review," *Women, sience and technology: A reader in feminist science studies*, pp. 46–52, 2001.

[3] S. Goldbeck-Wood, "Evidence on peer review—scientific quality control or smokescreen?," *BMJ: British Medical Journal*, vol. 318, no. 7175, p. 44, 1999.

[4] J. Huisman and J. Smits, "Duration and quality of the peer review process: the author's perspective," *Scientometrics*, pp. 1–18, 2017.

[5] C. T. Bergstrom and T. C. Bergstrom, "The costs and benefits of library site licenses to academic journals," *Proceedings of the National Academy of Sciences of the United States of America*, vol. 101, no. 3, pp. 897–902, 2004.

[6] G. E, "The history and meaning of the journal impact factor," *JAMA*, vol. 295, no. 1, pp. 90–93, 2006.

[7] G. Eysenbach, "Citation advantage of open access articles," *PLoS biology*, vol. 4, no. 5, p. e157, 2006.

[8] R. Walker and P. Rocha da Silva, "Emerging trends in peer review—a survey," *Frontiers in Neuroscience*, vol. 9, May 2015.

[9] B. Whitworth and R. Friedman, "Reinventing academic publishing online. part i: Rigor, relevance and practice," *First Monday*, vol. 14, no. 8, 2009.

[10] J. A. Evans and J. Reimer, "Open access and global participation in science," *Science*, vol. 323, no. 5917, pp. 1025–1025, 2009.

[11] V. Larivière, S. Haustein, and P. Mongeon, "The oligopoly of academic publishers in the digital era," *PloS one*, vol. 10, no. 6, p. e0127502, 2015.

[12] R. Van Noorden *et al.*, "The true cost of science publishing," *Nature*, vol. 495, no. 7442, pp. 426–429, 2013.

[13] M. Ware, "Peer review: benefits, perceptions and alternatives," *Publishing Research Consortium*, vol. 4, pp. 1–20, 2008.

[14] E. Ford, "Defining and characterizing open peer review: A review of the literature," *Journal of Scholarly Publishing*, vol. 44, no. 4, pp. 311–326, 2013.

[15] P. Frishauf, "Reputation systems: a new vision for publishing and peer review," *Journal of Participatory Medicine*, 2009.

[16] X. Shuai, A. Pepe, and J. Bollen, "How the scientific community reacts to newly submitted preprints: Article downloads, twitter mentions, and citations," *PloS one*, vol. 7, no. 11, p. e47523, 2012.

[17] Y. Benkler, "Degrees of freedom, dimensions of power," *Daedalus*, vol. 145, no. 1, pp. 18–32, 2016.

[18] A. Chaudhry, J. Crowcroft, H. Howard, A. Madhavapeddy, R. Mortier, H. Haddadi, and D. McAuley, "Personal data: thinking inside the box," in *Proceedings of The Fifth Decennial Aarhus Conference on Critical Alternatives*, pp. 29–32, Aarhus University Press, 2015.

[19] S. Bartling and B. Fecher, "Blockchain for science and knowledge creation. zenodo," *Publisher Full Text*, 2016.

[20] J. P. Tennant, J. M. Dugan, D. Graziotin, D. C. Jacques, F. Waldner, D. Mietchen, Y. Elkhatib, L. B. Collister, C. K. Pikas, T. Crick, *et al.*, "A multi-disciplinary perspective on emergent and future innovations in peer review," *F1000Research*, vol. 6, 2017.

[21] A. C. Kade Morton, "Aletheia: blockchain for scientific knowledge with a community management framework," 2017.

[22] V. Dhillon, "From bench to bedside: Enabling reproducible commercial science via blockchain," *Bitcoin Magazine*, 2016.

[23] M. Fuster Morell, *Governance of online creation communities: Provision of infrastructure for the building of digital commons*. PhD thesis, European University Institute, 2010.

[24] C. J. Lee, C. R. Sugimoto, G. Zhang, and B. Cronin, "Bias in peer review," *Journal of the Association for Information Science and Technology*, vol. 64, no. 1, pp. 2–17, 2013.

[25] A. Tenorio-Fornés, S. Hassan, and J. Pavón, "Open peer-to-peer systems over blockchain and ipfs: An agent oriented framework," in *Proceedings of the 1st Workshop on Cryptocurrencies and Blockchains for Distributed Systems*, pp. 19–24, ACM, 2018. .

[26] S. Ratnasamy, P. Francis, M. Handley, R. Karp, and S. Shenker, *A scalable content-addressable network*, vol. 31. ACM, 2001.

[27] R. C. Merkle, "A digital signature based on a conventional encryption function," in *Conference on the Theory and Application of Cryptographic Techniques*, pp. 369–378, Springer, 1987.

[28] J. Loeliger and M. McCullough, *Version Control with Git: Powerful tools and techniques for collaborative software development*. " O'Reilly Media, Inc.", 2012.

[29] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008.

[30] B. Benshoof, A. Rosen, A. G. Bourgeois, and R. W. Harrison, "Distributed decentralized domain name service," in *Parallel and Distributed Processing Symposium Workshops, 2016 IEEE International*, (Chicago, IL, USA), pp. 1279–1287, IEEE, 2016.

[31] V. Buterin, "Ethereum: A next-generation smart contract and decentralized application platform," 2014.

[32] N. Szabo, "Formalizing and securing relationships on public networks," *First Monday*, vol. 2, no. 9, 1997.

[33] P. De Filippi and S. Hassan, "Blockchain technology as a regulatory technology: From code is law to law is code," *First Monday*, vol. 21, no. 12, 2016.

[34] J. Peterson and J. Krug, "Augur: a decentralized, open-source platform for prediction markets," *arXiv preprint arXiv:1501.01042*, 2015.

[35] D. Larimer, N. Scott, V. Zavgorodnev, B. Johnson, J. Calfee, and M. Vandeberg, "Steem: An incentivized, blockchain-based social media platform," *March. Self-published*, 2016.

[36] M. L. Callaham and J. Tercier, "The relationship of previous training and experience of journal peer reviewers to subsequent review quality," *PLoS medicine*, vol. 4, no. 1, p. e40, 2007.

[37] P. Resnick, K. Kuwabara, R. Zeckhauser, and E. Friedman, "Reputation systems," *Communications of the ACM*, vol. 43, no. 12, pp. 45–48, 2000.

[38] E. Rajpert-De Meyts, S. Losito, and D. T. Carrell, "Rewarding peer-review work: the Publons initiative," *Andrology*, vol. 4, pp. 985–986, Nov. 2016.

[39] Z. Jan, A. Third, L.-D. Ibanez, M. Bachler, E. Simperl, and J. Domingue, "Sciencemiles: Digital currency for researchers," in *Companion Proceedings of the The Web Conference 2018*, WWW '18, (Geneva, Switzerland), pp. 1183–1186, International World Wide Web Conferences Steering Committee, 2018.

[40] B. Whitworth and R. Friedman, "Reinventing academic publishing online. part ii: A socio-technical vision," *First Monday*, vol. 14, no. 9, 2009.

[41] D. J. Solomon and B.-C. Björk, "A study of open access journals using article processing charges," *Journal of the Association for Information Science and Technology*, vol. 63, no. 8, pp. 1485–1495, 2012.

[42] B.-C. Björk, M. Laakso, P. Welling, and P. Paetau, "Anatomy of green open access," *Journal of the Association for Information Science and Technology*, vol. 65, no. 2, pp. 237–250, 2014.

[43] J. Benet, "IPFS-content addressed, versioned, P2p file system," *arXiv preprint arXiv:1407.3561*, 2014.

[44] E. Garfield, "The evolution of the science citation index," *International microbiology*, vol. 10, no. 1, p. 65, 2007.

[45] G. M. Sullivan and A. R. Artino Jr, "Analyzing and interpreting data from likert-type scales," *Journal of graduate medical education*, vol. 5, no. 4, pp. 541–542, 2013.

[46] A. E. Budden, T. Tregenza, L. W. Aarssen, J. Koricheva, R. Leimu, and C. J. Lortie, "Double-blind review favours increased representation of female authors," *Trends in ecology & evolution*, vol. 23, no. 1, pp. 4–6, 2008.

[47] S. Van Rooyen, F. Godlee, S. Evans, N. Black, and R. Smith, "Effect of open peer review on quality of reviews and on reviewers' recommendations: a randomised trial," *Bmj*, vol. 318, no. 7175, pp. 23–27, 1999.

[48] T. Groves and K. Khan, "Is open peer review the fairest system," *BMJ (Clinical research ed.)*, vol. 341, pp. 1082–1083, 2010.

[49] A. Schaub, R. Bazin, O. Hasan, and L. Brunie, "A trustless privacy-preserving reputation system," in *IFIP International Information Security and Privacy Conference*, pp. 398–411, Springer, 2016.

[50] R. L. Rivest, A. Shamir, and Y. Tauman, "How to leak a secret," in *International Conference on the Theory and Application of Cryptology and Information Security*, pp. 552–565, Springer, 2001.

[51] D. Chaum, "Blind signatures for untraceable payments," in *Advances in cryptology*, pp. 199–203, Springer, 1983.

[52] M. Blum, P. Feldman, and S. Micali, "Non-interactive zero-knowledge and its applications," in *Proceedings of the twentieth annual ACM symposium on Theory of computing*, pp. 103–112, ACM, 1988.

[53] E. B. Sasson, A. Chiesa, C. Garman, M. Green, I. Miers, E. Tromer, and M. Virza, "Zerocash: Decentralized anonymous payments from bitcoin," in *Security and Privacy (SP), 2014 IEEE Symposium on*, pp. 459–474, IEEE, 2014.

[54] M. De Rond and A. N. Miller, "Publish or perish: bane or boon of academic life?," *Journal of Management Inquiry*, vol. 14, no. 4, pp. 321–329, 2005.