DEPARTMENT OF INFORMATICS

TECHNISCHE UNIVERSITÄT MÜNCHEN

Master's Thesis in Informatics

Peer Review Verification with Verifiable Credentials and Zero-Knowledge Proofs

Kaan Uzdoğan

DEPARTMENT OF INFORMATICS

TECHNISCHE UNIVERSITÄT MÜNCHEN

Master's Thesis in Informatics

Peer Review Verification with Verifiable Credentials and Zero-Knowledge Proofs

Peer Review Beglaubigung mit Verifiable Credentials und Zero-Knowledge-Beweise

Author:	Kaan Uzdoğan
Supervisor:	Prof. Dr. Jens Großklags, Prof. Dr. Ali Sunyaev
Advisor:	Benjamin Sturm, Tibor Posa
Submission Date:	15 September 2021

I confirm that this master's thesis in informatics is my own work and I have documented all sources and material used.

Munich, 15 September 2021 Kaan Uzdoğan

Acknowledgments

Without doubt the very first name here is my father Musa Kazım Uzdoğan, who lost his fight to COVID-19 at the very beginning of this thesis. He with my mother Ayşegül Uzdoğan have been my biggest supporters throughout my life and put everything they had for me to become successful. Definitely, I am standing on the shoulders of giants. I know you would be extremely proud to see me achieve this. We will be loving and remembering you forever. I am also thankful for having a larger family who always showed their love and support through the difficult times.

Secondly, big thanks to my advisor Benjamin Sturm for his guidance and great communication throughout this work. I really enjoyed our discussions and appreciate your extensive feedback each time we met, although always virtually. I would also like to thank Prof. Ali Sunyaev and Prof. Jens Großklags for providing me the opportunity to work on this topic, and Tibor Posa for his reviews. Another mention goes to my colleagues at Max Planck Digital Library where I was working on the project bloxberg. Particularly to James Lawton, who introduced me to this problem and whom I enjoyed closely working with a lot. Also, I want to thank all interviewees for taking their time and providing valuable insights: João Pedro Oliveira, Tiago Paixão, Kevin Wittek, and two pseudonymous interviewees.

Finally, even though we never met, I want to commemorate Jon Tennant here, a great communicator and a tireless proponent of open science whose loss shocked many. I benefited and influenced by his works to a great extent, and the legacy he left helped me shape this work a lot.

Abstract

Peer review is an essential part of scientific publishing and scientific knowledge creation. Despite the acknowledged importance, current incentives in scientific publishing are not towards doing peer reviews but instead to publish more peer reviewed papers. The process itself is also shown to have problems such as bias, inconsistency, and ineffectiveness. The community generally agrees that it can be improved by increasing the recognition and incentives for peer reviews. Often, reviews are blinded and cannot be published which makes it is difficult to credit the reviewers for their work. Peer review recognition platforms such as Publons try to solve this problem by acting as trusted third-parties verifying reviews and letting researchers build a peer review resume. However, the ownership of this data under a single commercial entity might have unwanted consequences from an open science perspective, in particular the availability and the transparency of the data. These concerns became more evident with the acquisition of Publons by Clarivate Analytics. It is of benefit to avoid the mistakes made in the scientific publishing that resulted with centralization and limited access to information.

Recently a specification called Verifiable Credentials became an official W3C recommendation. It is claimed to enable credential exchange in a secure and privacy-preserving way by selective disclosure of claims and zero-knowledge proofs which let proving a statement without having to share the underlying data. This Design Science Research work is aimed to explore the verification of closed reviews without a trusted third-party using these recent technologies. The designed system also proposes a peer review showcasing system similar to Publons. A working prototype is implemented using the existing tools and libraries to demonstrate the feasibility of the design. The finished design is evaluated for the self imposed requirements and through five qualitative interviews with researchers that have reviewing experience. Based on the findings an acceptance model for the designed system is proposed.

Contents

1 Introduction

Peer review is the formal process of the evaluation of scholarly works by people specialized in the subject of the work (Moxham & Fyfe, 2018, p. 864). Common applications of peer review in scientific research are the selection of grant and fellowship applications, and the selection of manuscripts for scientific journals. In academic publishing when a researcher submits an academic paper for publication, journal editors ask "peers", who are experts in the field to scrutinize the paper. Based on these reports the editor either rejects the paper, sends the paper back to the author for revision, or accepts it for publication. By determining what gets published or who gets funding, reviewers act as gatekeepers of science and the process ensures the quality and soundness of the scientific work (Bornmann, 2011).

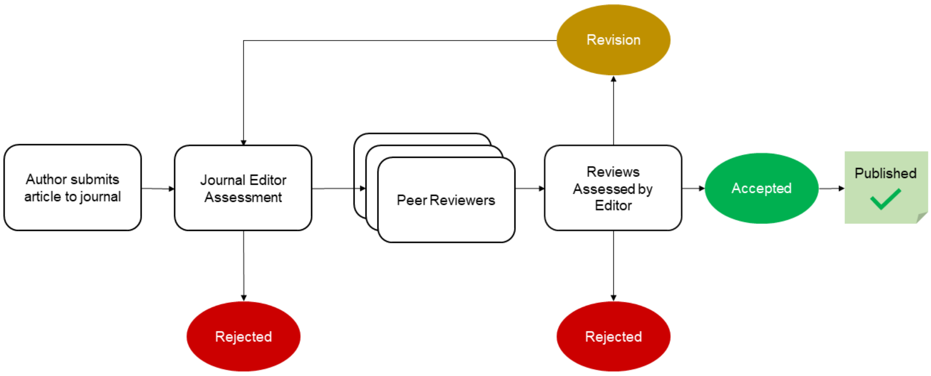

Revision
Author submits article to journal
Journal Editor Assessment
Peer Reviewers
Reviews Assessed by Editor
Accepted
Published
Rejected
Rejected

Figure 1.1: The publishing process

Peer reviews can be classified by how the identities of parties are managed. In a double-blind review, only the editor knows the identities of the author and the reviewer. In a single-blind review, the name of the reviewer is hidden from the author to let the reviewer criticize without worrying about personal relationships or conflict of interests. The third and emergent form of the peer review is open peer review where the identities of both author and the reviewer are known to each other. In some forms of the open peer review, the identities and the review reports are also publicly available (Horbach, S. P. J. M. & Halffman, 2017, p. 4), and therefore reviewers can gain credit for their work. Although, the term "open peer review" not only encompasses the openness of identities and the content, but also used for the open participation and transparency of the whole process (Ross-Hellauer, 2017).

Peer review takes place in many different forms and employs different processes and it's difficult to acknowledge it as a single system (Horbach, S. P. J. M. & Halffman, 2017, p. 2). But its essence and rationale are shared among all different applications. Emerged among earlier scientific societies as an internal scrutiny for the scientific quality of manuscripts, it held its importance throughout the proliferation of the printing press, globalization of science after World War II (Fyfe, Coate, Curry, et al., 2017), and the adoption of information technologies. It is still perceived by some as the gold standard in scientific publishing (Mayden, 2012) and provides legitimacy for the generated knowledge (J. P. Tennant & Ross-Hellauer, 2020).

1.1 Problem Statement

It is widely accepted that peer review plays an important role in research (Publons, 2018; Taylor & Francis, 2015; Ware, 2008; Zuckerman & Merton, 1971). Despite its importance, peer review is shown to be far from being perfect, by being prone to biases (Lee, Sugimoto, Zhang, & Cronin, 2013; Mahoney, 1977), inconsistencies (Peters & Ceci, 1982; Rothwell & Martyn, 2000), and being ineffective in detecting errors (Schroter, Black, Evans, et al., 2004). It usually takes 3 to 5 hours (Mulligan, Hall, and Raphael, 2013, p. 146; Ware, 2008, p. 42) to complete a review and it usually takes more than 3 months for a paper to be accepted (Ware, 2008, p. 51). The process is often slow for authors and time consuming for reviewers. Reviewers who are academics themselves with various duties are often not compensated for their review work and they don't receive credit for their work. Given that number of publications is growing each year (Bornmann & Mutz, 2015) and each manuscript typically requires 2 to 3 reviewers the peer review system is being put under growing pressure. This situation is said to cause "reviewer fatigue" (Breuning, Backstrom, Brannon, et al., 2015). At the same time, editors are reporting that it is getting more difficult to find suitable reviewers, indicated by the increasing decline rates to review invitations (Baveye & Trevors, 2011; C. W. Fox, Albert, & Vines, 2017).

Despite the numerous deficiencies of the process, it is argued that there is no consensus on an alternative (R. Smith, 2006; S. N. Young, 2003) and it is currently the best method ensuring the soundness of scientific publishing (Grainger, 2007, p. 5201; Horbach, S. P. J. M. and Halffman, 2017, p. 2). A range of innovations aimed to tackle the stated problems failed to provide a cure and the peer review remains mostly unchanged (J. P. Tennant, Dugan, Graziotin, et al., 2017).

Problem 1: Peer Review Lacks Incentives

Some of the problems of peer review mentioned above are believed to be results of the lack of incentives to review (Derraik, 2015; Willis, 2016), and there's an ongoing discussion on how to increase researchers' engagement in reviews in the light of these problems (Derraik, 2015; Gasparyan, Gerasimov, Voronov, & Kitas, 2015; Hauser & Fehr, 2007; Squazzoni, Bravo, & Takács, 2013). The lack of incentives has its roots within that today the measures and indicators of academic performance are the number of papers published, number of citations, or other citation based scientometrics. These measures play an important role in deciding who climbs up the ranks, who gets hired, or who receives the funding. Despite its importance, peer reviews usually are not recognized as a research output as the manuscripts and do not contribute to researchers' perceived academic performance (J. P. Tennant, Dugan, Graziotin, et al., 2017). Therefore, researchers are disincentivized to do reviews and incentivized to publish more manuscripts.

The reliance on publishing-related metrics has also other consequences on peer reviewing. The state of affairs creates the mindset of "publish or perish": the constant pressure to publish more and get cited more (Rawat & Meena, 2014). Yet, the way to publish more and get cited more is not only doing more research. One can publish the results of their work in smaller and less coherent slices (Ferreira, Bastille-Rousseau, Bennett, et al., 2016, p. 4) in an act called "salami publication" (Supak Smolcić, 2013). The act is considered unethical (Supak Smolcić, 2013, p. 238) and with each paper reviewed by multiple reviewers, it puts more pressure on the peer review system (Ferreira, Bastille-Rousseau, Bennett, et al., 2016, p. 4). This effect is amplified when a paper gets redundantly reviewed in different journals i.e. when authors go "journal shopping". In this case, following a rejection by a journal with a higher impact, authors continue submitting their papers to gradually lower impact journals until their papers get published while the new editors and reviewers of the submitted paper are not aware of the previous reviews done (Kovanis, Porcher, Ravaud, & Trinquart, 2016, p. 10).

If everyone publishes more and reviews less, then who is doing all the reviews? A strong imbalance in the peer review system was observed where a larger percentage of the peer reviews are done by a minority of researchers and thanks to them there is a sufficient supply of reviewers (Kovanis, Porcher, Ravaud, and Trinquart, 2016; Petchey, Fox, and Haddon, 2014; Ware, 2008, p. 37). Those "peer-review heroes" bear the burden by reviewing much more than they publish (Kovanis, Porcher, Ravaud, & Trinquart, 2016, p. 9). The situation raises the concerns that the system may be in a "tragedy of the reviewer commons" (Hochberg, Chase, Gotelli, et al., 2009) where participants of the system are encouraged to exploit the system by submitting more papers and less incentivized to do peer reviews. By incentivizing peer reviews it can be possible to attract more reviewers to the reviewer pool. This would also help balance the heavy burden placed on the reviewing system potentially letting editors find reviewers easier and shorten the time taken from submission until the publication of a manuscript.

There's a consensus among researchers that an improvement in peer review incentives and higher recognition would enable better reviews (Publons, 2018). Still, it is not clear how to incentivize peer reviews (Ware, 2008, p. 28, Warne, 2016, Gasparyan, Gerasimov, Voronov, and Kitas, 2015, Tite and Schroter, 2007) and how to evaluate and reward good peer reviews (Ferreira, Bastille-Rousseau, Bennett, et al., 2016, p. 12). Notwithstanding, the nature of peer reviews makes it impossible to attribute reviews to their authors and impairs the recognition and incentivization aspects (J. P. Tennant, 2018, p. 4).

Problem 2: Closedness of Reviews Prevents Their Acknowledgment

The practice of blinded reviewing is a feature of the process that hinders public review acknowledgement. Today most of the peer reviews are done as single or double-blind (Wolfram, Wang, Hembree, & Park, 2020). Even though open peer review seems to be gaining popularity (Wolfram, Wang, Hembree, & Park, 2020), scientists are more likely to accept review requests when their identities are hidden (van Rooyen, Godlee, Evans, et al., 1999) and majority of the researchers still prefer blinded reviews over open peer reviews (Mulligan, Hall, and Raphael, 2013, p. 149; Taylor & Francis, 2015; Wolfram, Wang, Hembree, and Park, 2020, pp. 1038–1039). It is likely the majority of peer reviews will remain blinded as the anonymity is considered necessary for strong and unbiased scrutiny (Ross-Hellauer, 2017, pp. 21–23).

However, a problem the closedness of reviews introduces is the difficulty to verify and accredit reviews. Since the whole review process takes place internally in journal management systems it is not possible to find out externally if a researcher has really done a peer review for a specific manuscript or a journal, without explicitly contacting the journal. In most of the cases, the transaction costs of contacting a journal is too large for a review, as virtually none of the journals have such a verification system. For reviewers to gain recognition for their work, it is essential that they can easily prove the authenticity of their reviews. The researchers may then showcase their review works done for specific journals and articles publicly or present them when needed as a demonstration of expertise in a field e.g. in job and grant applications. It may also highlight the reviewing workloads of researchers to their employers (Raoult, 2020, p. 2).

If the closed peer reviews can be verified and recognized, these records can be embedded in alternative peer review metrics. Employers are increasingly resorting more to citation-based metrics for assessing their researchers (Bianchi, Grimaldo, & Squazzoni, 2019; Cantor & Gero, 2015; Kachewar & Sankaye, 2013; Veríssimo & Roberts, 2013). Peer review metrics may be taken into account when assessing academic performance (Ferreira, Bastille-Rousseau, Bennett, et al., 2016, p. 11).

Problem 3: Existing Peer Review Showcase Platforms Do Not Align with the Open Science Goals

The above problem caught the attention of what is called "peer review showcasing platforms". There are already running projects that aim to bring recognition to peer reviews by letting reviewers showcase their work. Since the review data is not publicly available, these platforms can track the review contributions of a researcher for them, and verify the reviews they add to their profiles. By providing this verification service, they act as a trusted third party between the reviewers and and the bodies potentially interested in this information such as editors, funders, universities or agencies.

One such platform, Reviewer Credits[1] is a project to let reviewers certify peer review activity, display their review records, and earn rewards such as books, and discounts to paid publishing services. Reviewers can claim their activity either through automated data transfer between the platform and journal or by Reviewer Credits manually contacting the publisher. ORCID[2] also lets users add reviews to their profiles from open review journals or if the journal is a paid ORCID member and provides review data to the platform though its API (Therese, 2018). The more popular platform providing a similar service is Publons. Founded by Andrew Preston and Daniel Johnston in New Zealand in 2012 it quickly gained popularity and was welcomed by many academics (D. R. Smith, 2015, p. 266) and was eventually acquired by Clarivate Analytics in 2017. As of November 2020, Publons claims to have over 2 million members (Publons, 2020). On Publons, researchers can create a profile and add the reviews they have done. To add a peer review, they can either follow a link provided by the journal with a Publons integration after submitting their review or they can manually forward their review acceptance emails to Publons, who then manually verifies the review. By gathering publications and reviews, researchers can showcase their scholarly efforts and earn badges and awards such as “Top Reviewer” or “Highly Cited”.

[1] https://www.reviewercredits.com

[2] https://orcid.org

These platforms help researchers gain credit for their review contributions, but the commercialization of the domain (J. P. Tennant, Dugan, Graziotin, et al., 2017, p. 14), and the proprietary status and of the review showcasing platforms may not be well aligned with the open science goals. Open science is a broad term used for different aspects of science and how science is conducted and there are different definitions of the term. Vicente-Saez and Martinez-Fuentes, 2018 define it as knowledge generation with the four characteristics: transparent, accessible, shared, and collaborative by analyzing the use of term throughout the literature. Pontika, Knoth, Cancellieri, and Pearce, 2015 created a taxonomy by braking down the the broader term "open science" into hierarchical components to provide a consistent terminology and to map the concepts around open science. Fecher and Friesike, 2013 identify five schools of thought under the open science discourse, each aims for "opening" different aspects of the knowledge creation process.

- **Public School:** Open participation of the knowledge creation process, making science comprehensible for common citizens.
- **Democratic School:** Accessibility and transparency for the created knowledge: Open Access, Open Data
- **Pragmatic School:** Improving collaboration, stimulating knowledge dissemination.
- **Infrastructure School:** Providing researchers open tools for dissemination and collaboration
- **Measurement School:** Finding new ways to measure researchers' impact, recognizing formerly invisible scientific contributions

Overall, open science aims to increase the rigour, accountability, and reproducibility in research and "to make research more open to participation, review/refutation, improvement and (re)use for the world to benefit" (Bezjak, Clyburne-Sherin, Conzett, et al., 2018).

Despite Publons being accepted by many scientists, it's pointed out that its metrics may be biased (Ortega, 2019), and it may be failing to distinguish authentic reviews (Teixeira da Silva, 2020). Current verification process by Publons, in particular the verification through review receipt emails, is not transparent. Publons lets users add reviews to their profiles by forwarding the "Thank you for your review" responses of journals. An email response is an easily forgeable and unverifiable message. There are no studies on the peer review data if this problem is practically relevant, but there exist fake reviews (Qi, Deng, & Guo, 2017; RetractionWatch, 2015; Teixeira da Silva, 2017) and predatory journals wanting to exploit scientific metrics (Demir, 2018; Xia, Harmon, Connolly, et al., 2015), and credential fraud in

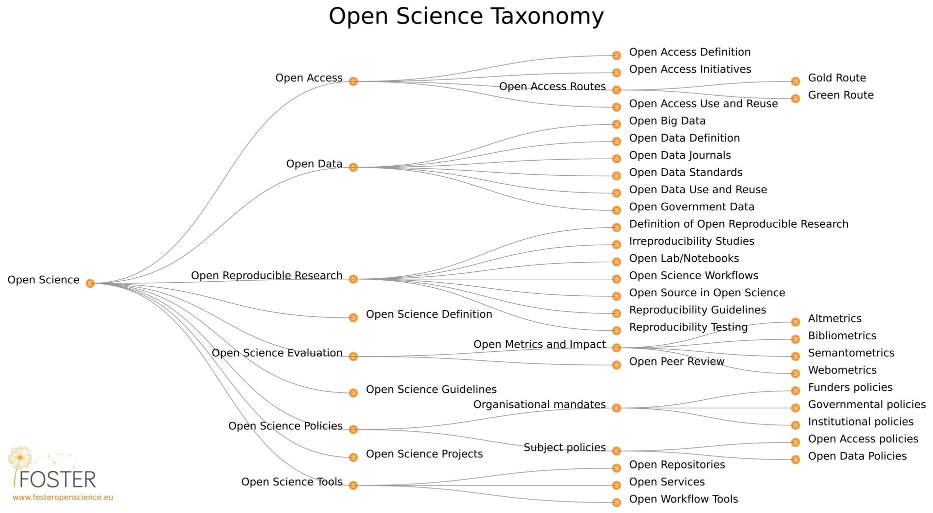


Figure 1.2: (Pontika, Knoth, Cancellieri, & Pearce, 2015)

science is well known (Wilson, 2020). Besides, on Publons it is not possible to see how the verification is done and there is no distinction on the platform between an email verification and a verification through a journal integration. Effectively, Publons has to be trusted for the data they provide.

Besides, the fact that the data on the platform is owned by Publons, and effectively Clarivate Analytics, brings the accessibility of the data into question. The platform's provided API does not provide much data and existing studies making use of the Publons data extract it using web crawlers (Ortega, 2017, p. 952) which is not allowed without Publons' written consent according to the platform's terms (Publons, 2014). The platform appears to have provided data to researchers when requested (Kovanis, Porcher, Ravaud, & Trinquart, 2016, p. 12), however there are no guarantees that the data will remain freely accessible as long as it is owned by a proprietary company. Concerns have also been expressed for the transparency of the data previously provided by Clarivate Analytics (Rossner, van Epps, and Hill, 2007; Teixeira da Silva and Al-Khatib, 2019, p. 3), as the provider of the Journal Impact Factor, and for the fairness of its practices (Teixeira da Silva, 2013). A non-profit may be better suited for keeping this data open and accessible. Currently in the case of ORCID, which is a non-profit, the journals need to become paid ORCID members and integrate their API to be able write the review contributions of the researchers.

The aggregation of peer review data by proprietary parties might also be inappropriate for publishers and journals. The journals are effectively giving away their valuable review data to Publons for free. In turn, Clarivate Analytics processes this data and makes use of it for their profit. An example is the editor matching tool Publons has that lets editors find suitable matches for peer reviews of a manuscript[3]. This itself may not be undesirable, as the fees may be justified by the value it provides for its users. But a single party aggregating the data has a higher risk of causing disagreements with publishers. If a publisher is unwilling to provide review data to a potential competitor, this may hinder the review coverage of the platform. Ideally, a platform should remain an open non-profit, or a joint organization governed by different stakeholders of the whole peer review ecosystem.

The problems of centralization in publishing is apparent (Larivière, Haustein, & Mongeon, 2015) and there is ever more demand for open science (Piwowar, Priem, Larivière, et al., 2018, pp. 1–3). As long as the world's peer review data is under the control of a single party, there exists the possibility for the sole owner of the data to restrict access to it, or start charging fees. This privileged position of the showcasing platforms are due to the role they play as trusted third parties in review verification. If these third parties can be disintermediated, and direct trust can be established between reviewers and consumers of the review data, a review showcasing system with more transparency, open standards, and open data may be possible.

1.2 Research Question

Peer review is a broad and controversial topic with many conflicting perspectives. The process also has many problems outlined that is interconnected with the other aspects of scientific epistemology and the current scientific publishing specifically. It is important to have a narrow focus to be able to analyze the specific problems and to bring impactful solutions. As stated in Problem 3, there are already platforms aiming to bring recognition to peer reviews however proliferation of such showcasing platforms may have unwanted consequences from an open science perspective. Since their ability to withhold data stems from their position as a trusted third-party, this aspect constitutes the root problem. To find a solution to this practical problem, the following research question needs to be investigated:

How can closed peer reviews be verified without trusted third-parties?

1.3 Research Problem

The incentivization problem (Problem 1) in peer review caught the attention of scientists and was studied in more detail relatively. Besides the descriptive literature on peer review's

[3] https://publons.com/benefits/reviewer-connect

shortcomings, a variety of works discussed and prescribed solutions to the incentive problem. An often encountered suggestion is to ask researchers to do sufficient reviews to balance the system, usually 3 reviews per paper, a "quid pro quo" (Derraik, 2015, Grainger, 2007, p. 5201). To maintain the timeliness of the process Hauser and Fehr, 2007 suggest a punishment for reviewers who return their reviews late and a reward for the ones returning on time. Ferreira, Bastille-Rousseau, Bennett, et al., 2016 suggest making peer review mandatory and paying the reviewers and calls for a decoupling of the peer review system from the scientific publishing by founding a Global Peer Review Platform. Direct monetary compensation of reviewers was also suggested many times (Prüfer & Zetland, 2010). J. Fox and Petchey, 2010 suggest a credit system where authors have to pay for their submissions and earn by conducting reviews, effectively "privatizing the reviewer commons". Others proposed crypto-economic models through peer review tokens on a blockchain that will work as credits for peer reviews or as reputation indicators (Avital, 2018; Jan, Third, Ibanez, et al., 2018; Spearpoint, 2017; Tarkhanov, Fomin–Nilov, & Fomin, 2020). Also using a blockchain-based token and lotteries Janowicz, Regalia, Hitzler, et al., 2018 provide a model for how integrating distributed ledger technologies could benefit the Semantic Web journal's processes. Tenorio-Fornés, Jacynycz, Llop-Vila, et al., 2019 suggest a whole publishing system that is decentralized using Ethereum and IPFS. Ants-Review suggests an Ethereum based incentive system with its native token ANTS that allows bounties for open anonymous peer reviews (Trovò & Massari, 2021). However, these works either assume the reviews to be open, or only high level suggestions that don't consider how to collect and verify the peer review data, which leads to the second problem.

The second problem is the focus of the mentioned showcasing platforms. Additionally, the proponents of open peer review also argue that open identities in peer reviews would allow the recognition of peer reviews (Ross-Hellauer, Deppe, & Schmidt, 2017, p. 3). Although there is an increasing interest (Wolfram, Wang, Hembree, & Park, 2020), the larger scientific community seems hesitant to move to an open identities peer review system (Ross-Hellauer, Deppe, & Schmidt, 2017; Taylor & Francis, 2015; Ware, 2008). With that, currently the only viable solution to peer review recognition seem to be the showcasing platforms. Publons, being the most popular, has been welcomed by the scientists but following their acquisition by Clarivate Analytics, questions has been raised about the commodification of the peer review data (J. P. Tennant, Dugan, Graziotin, et al., 2017, p. 14, Teixeira da Silva and Al-Khatib, 2019). As discussed, this also presents potential unwanted consequences in terms of open science. There doesn't seem to be any works in the literature considering the third problem and attempting to circumvent the third-parties in peer review verification.

1.4 Goal

The main goal of this work is to design a system that will enable the verification of closed peer reviews without a trusted third-party. As an artifact that will improve upon the existing showcasing platforms, the designed system shall also let reviewers showcase their records. Additionally, the technical feasibility of the conceptual design with the existing technologies should be demonstrated with an implementation.

1.5 Methodology

As the work is exploratory and it is goal is to create an improved artifact that will enable the verification of closed peer reviews without a trusted third-party, it was suitable to structure the research process according to a design science framework. For this work the Design Science Research Methodology (DSRM) proposed by Peffers, Tuunanen, Rothenberger, and Chatterjee, 2007 was taken as a guideline for conducting research. The proposed framework presents a nominal process model that can be followed when conducting design science research in information systems. The authors suggest dividing the research process into 6 steps as shown in Figure 1.3. The process is not necessarily linear. During the research, the knowledge generated when creating the artifact can be used to refine and improve the artifact, and the improvement of the artifact yields more applicable knowledge. This cycle may be repeated multiple times until the artifact reaches the desired state. Additionally, it is possible to start the research process from the four entry points:

- **Identify Problem & Motivate:** Problem-Centered Initiation
- **Define Objectives of a Solution:** Objective-Centered Solution
- **Design & Development:** Design & Development Centered Initiation
- **Demonstration:** Client/Context Initiated

A problem-centered initiation was adopted for the research process of this work.

Problem Identification

Problem identification was the starting point of the research and the *peer review incentive problem* was the focus initially. The problem statement is given in detail in Section 1.1 but here the research path to the final research question will be given. Initially, during my work

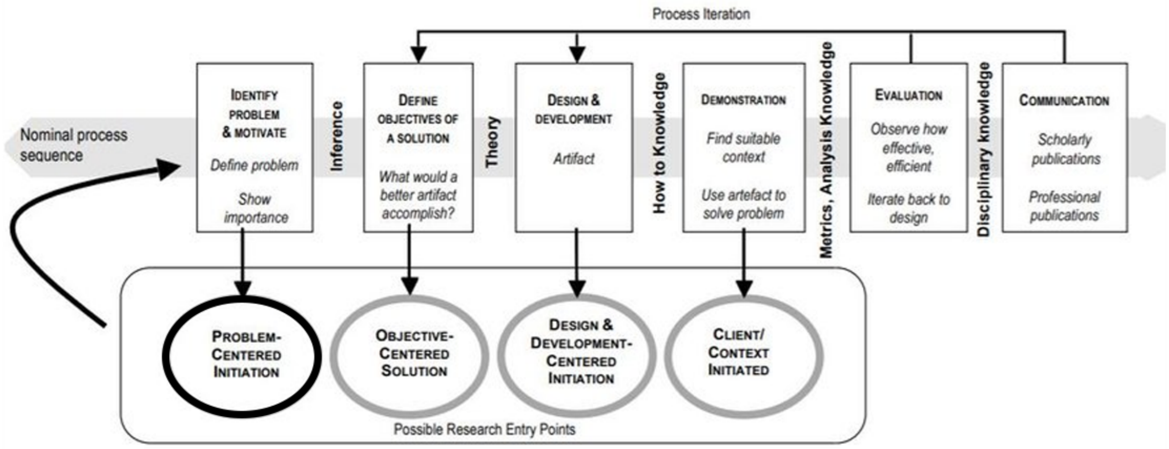

Process Iteration
Nominal process sequence
IDENTIFY PROBLEM & MOTIVATE
Define problem
Show importance
Inference
DEFINE OBJECTIVES OF A SOLUTION
What would a better artifact accomplish?
Theory
DESIGN & DEVELOPMENT
Artifact
How to Knowledge
DEMONSTRATION
Find suitable context
Use artefact to solve problem
Metrics, Analysis Knowledge
EVALUATION
Observe how effective, efficient
Iterate back to design
Disciplinary knowledge
COMMUNICATION
Scholarly publications
Professional publications
PROBLEM-CENTERED INITIATION
OBJECTIVE-CENTERED SOLUTION
DESIGN & DEVELOPMENT-CENTERED INITIATION
CLIENT/ CONTEXT INITIATED
Possible Research Entry Points

Figure 1.3: Design Science Research Methodology framework proposed by Peffers, Tuunanen, Rothenberger, and Chatterjee, 2007

at Max Planck Digital Library's bloxberg[4] that involves peer reviews and blockchains, I was introduced to the peer review incentive problem. This was followed by research in peer review, mainly in terms of metascience. A literature review brought some central works on the state of art of the peer review and its problems (Bornmann, 2011; Ferreira, Bastille-Rousseau, Bennett, et al., 2016; Horbach, S. P. J. M. & Halffman, 2018; Kovanis, Porcher, Ravaud, & Trinquart, 2016; Moxham & Fyfe, 2018; Publons, 2018; Ross-Hellauer, 2017; Ross-Hellauer, Deppe, & Schmidt, 2017; J. Tennant, 2018; J. P. Tennant, Dugan, Graziotin, et al., 2017; Ware, 2008). All resources were categorized individually and with excerpts in the Citavi resource management software for future reference. The literature review uncovered the individual problems in peer reviewing such as its quality, the long duration of the review process, and the increasing rejection rates, and that these problems can be traced back to the lack of incentives to do peer reviews. Solution proposals in the literature can be categorized in two groups: the ones that propose monetary incentives for doing peer reviews, and the proposals that focus on bringing recognition to the review contributions of researchers. The latter is also a prerequisite for the former as identification and verification of reviews are needed to be able to reward appropriately. This also brought into light the inherent dilemma of the peer review between keeping the reviews objective and unbiased, and making the process transparent and accountable, which stems from the practice of blinded reviews. Further, it revealed that the lack of recognition to peer reviews is due to the nature of the process, that the identities

[4] https://bloxberg.org

and contents of peer reviews are hidden and not shared publicly. Further research was led to the platforms that aim to bring recognition to both open and closed reviews, namely the *peer review showcasing platforms* e.g. Publons.

Even though these platforms provide value to their users, concerns about Publons were identified. Also from an open science perspective and considering the practices of the centralized large publishers (Larivière, Haustein, & Mongeon, 2015), problems related to transparency and centralization, and potential practices by the platform undesirable in terms of open data and open access were identified. Finally, it is pinpointed that these originate from the role these platforms take as *trusted-third party* verifiers, and the research question and the main goal was derived specifically from this.

Defining Objectives

Considering the outlined problems, the main goal of the work was defined as designing a system that will enable the verification of peer reviews without a trusted third party. Additionally, to design an artifact that achieves the main goal of the work, and that is in line with the open science goals, a set of requirements the designed artifact should satisfy were defined. How and why these requirements were defined is illustrated in the Section 3.1.

Design and Development

Based on the requirements the artifact was designed using the Verifiable Credentials and Zero-Knowledge Proofs that allows the verification of closed reviews without a trusted third-party. Initially the stakeholders of such a system was defined and the interactions between them were outlined on a high level (Figures 3.1, 3.2). Here, as an open standard that allows verification, and extensibility Verifiable Credentials was chosen as the basis. Also, the supported zk-proofs signature schemes allow the selective disclosure of the attributes, which is a requirement of the system and a part of stakeholder interactions. Accordingly, the BBS+ signature scheme was chosen. Following, a JSON-LD vocabulary for peer reviews was defined and example peer review credentials were created. The vocabulary and the examples were updated several times to fit the use case, but was kept minimal to assume a basic peer review process. The interactions between the reviewer and journal, i.e. the peer review credential issuance was outlined. Different DID methods were considered for the identification of parties and the verification of the credentials. Additionally, a showcasing platform was described that allows the aggregation of reviews and lets researchers build a peer review resume.

Demonstration

A working prototype was developed using Node.js, React, Mongodb, and the existing VC and zk-proofs toolkits, which demonstrates the technical feasibility of the designed artifact. The code of the prototype was open sourced and the applications were deployed to Heroku. An overview of the architecture of the prototype was given. How users can interact with it was also demonstrated.

Evaluation

Initially, the system was evaluated for the compliance with the defined requirements. Additionally, five interviews with researchers with peer reviewing experience was conducted to evaluate the designed system. The one hour interviews were recorded at interviewees' consent and were transcribed using an AI assisted transcription tool. Key insights for the user behavior and the evaluation of the system were extracted and grouped. Based on these insights, an acceptance model for the designed system was proposed.

Communication

Finally, the work is communicated in the form of a thesis document, and the open source code is shared on GitHub with instructions how to use the deployed prototype.

1.6 Structure

The rest of this work is structured as follows: Chapter 2 (Background) introduces the technical foundations in this work that are required for the creation of and to understand the proposed solution. Chapter 3 (Design & Implementation) outlines the requirements defined for the designed artefact and describes the design of the proposed system. Here the details of the artefact are laid out and the design decisions are communicated. Next in this chapter, the implemented prototype is described, which demonstrates the technical feasibility of the conceived design. A comparison between the conceptual design and the implemented prototype is also provided. Chapter 4 (Evaluation) involves the evaluation of the designed artefact based on the interviews with researchers. Chapter 5 (Discussion) shares the learnings gained in the process, and discusses potential future work and considerations. Finally, Chapter 6 (Conclusion) presents the conclusions.

2 Background

2.1 Verifiable Credentials

Verifiable Credentials (VC) is a recent W3C standard for interoperable digital credentials on the Web that is cryptographically secure, tamper-evident, privacy respecting, and machine-verifiable" (Sporny, Longley, & Chadwick, 2019). These credentials include but are not limited to passports, ID cards, university degrees, tickets etc. Any set of claims about a subject can be a credential. In the VC setting these claims create *subject-property-value* relationships that can be expressed in graphs. For instance being graduated from a university can be represented as the graph in Figure 2.1.

Subjects of claims are not necessarily persons and can be anything. In a peer review context a claim could be *Peer Review-author-John Doe* where the subject is the peer review. Alternatively same relationship can be represented as *John Doe-reviewerOf-Peer Review* where the subject is the person.

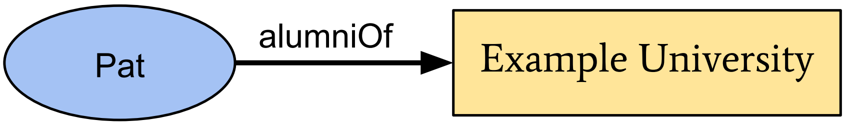


Figure 2.1: Example subject-property-value relationship of a graduation claim (Sporny, Longley, & Chadwick, 2019)

Although people usually associate credentials to be issued only by a respected authority such as a state, a university or a hospital, Verifiable Credentials allows anyone to issue claims. Yet, each credential is meaningful in a certain context and depending on the trust relationships between parties. An *alumniOf* claim is only meaningful if issued by a university that is known to the employer in a job application or a *goodHusband* claim only makes sense if issued by a spouse. Parties that receive a credential can choose to accept or reject a credential depending on the real world trust relationships.

A credential is a set of claims, i.e. a graph of information around a subject. Additional to the claims, the metadata and a digital proof form a verifiable credential. The proof is generally a digital signature of the claims and metadata, which makes the verifiable credential "verifiable".

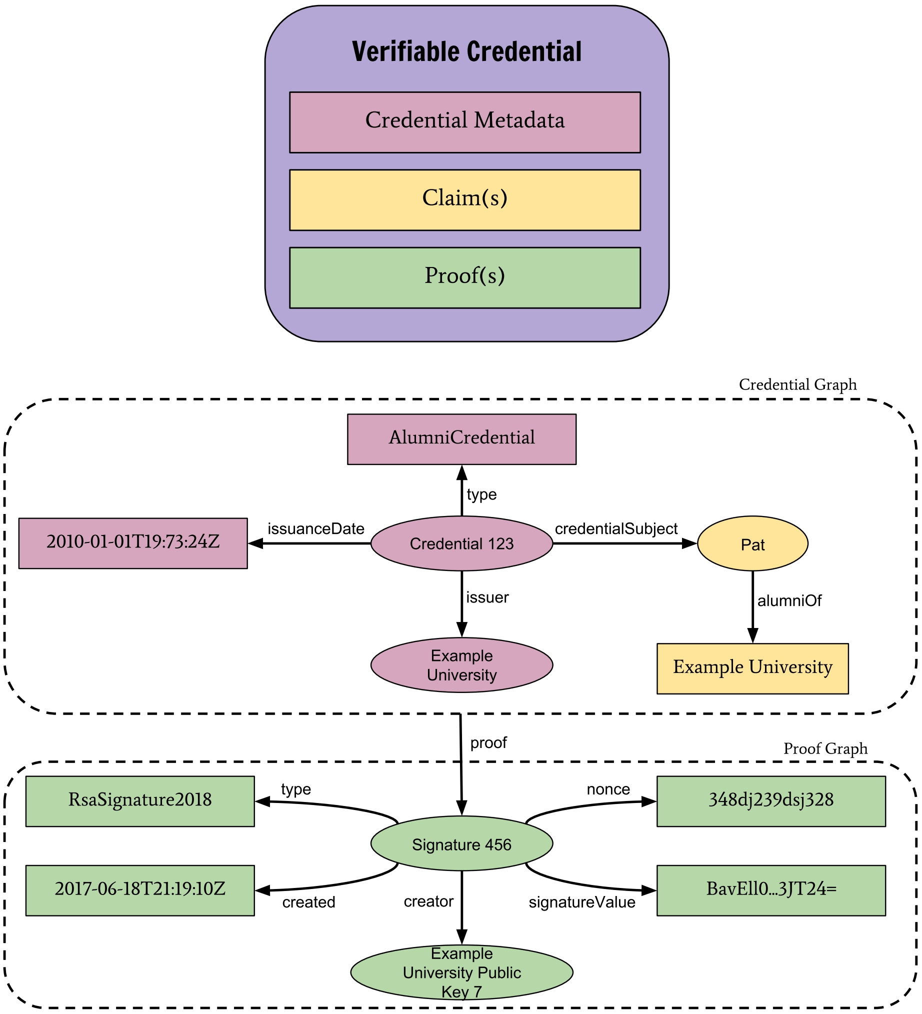


Figure 2.2: Components of a verifiable credential and the graph of information of an example credential (Sporny, Longley, & Chadwick, 2019)

The VC specification models the stakeholders and interactions between them as in Figure 2.3. *Issuer*s assert claims and issue credentials about subjects, *Verifier*s verify the credentials presented to them, and *Holder*s acquire, store, and present credentials. Note that the subject of a credential can be different than its holder such as a pet being the subject and its owner being the holder, or a peer review as the subject and the reviewer as the holder. Finally, a

Verifiable Data Registry acts as the backend of these interactions by maintaining identifiers and schemas. This registry could be a distributed ledger or a central database depending on the implementation.

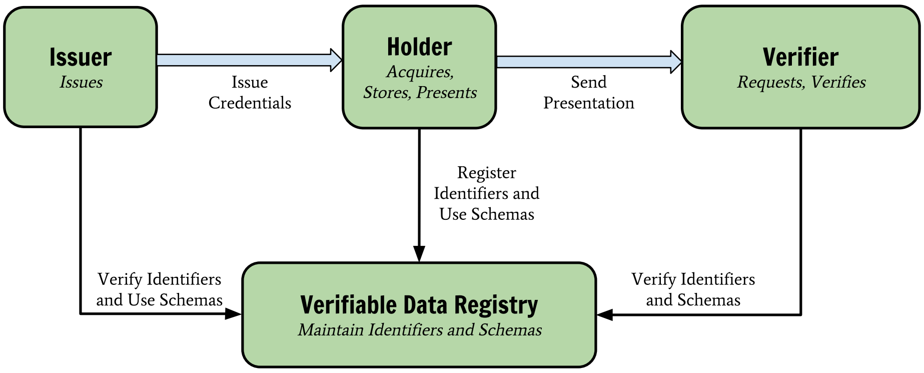

Issuer
Issues
Issue Credentials
Holder
Acquires, Stores, Presents
Send Presentation
Verifier
Requests, Verifies
Register Identifiers and Use Schemas
Verify Identifiers and Use Schemas
Verifiable Data Registry
Maintain Identifiers and Schemas
Verify Identifiers and Schemas

Figure 2.3: Stakeholders of a Verifiable Credentials ecosystem and their roles (Sporny, Longley, & Chadwick, 2019)

2.1.1 Verifiable Presentations

The specification also describes an extension to the VC data model that enables the packaging of multiple credentials and verification of the authorship of the data. A Verifiable Presentation consists of one or more verifiable credentials, presentation metadata, and a proof which is usually a digital signature of the first two. Credential holders can combine different credentials from different issuers for each use case, and the proof of the presentation provides the means to verify the authorship of data that the credentials are being presented by their intended holders and not someone else.

2.1.2 Syntax

The data model provided in the VC specification is an abstract representation of the information around a credential. For the exchange of the information a machine readable data exchange format or syntax is required. Popular data exchange formats are XML (Rose, Hollenbeck, & Masinter, 2003), JSON (Bray, 2017), and YAML (Ben-Kiki, Evans, & döt Net, 2009). Although any syntax can be used, the specification describes JSON Linked Data (JSON-LD) (Sporny, Longley, Kellogg, et al., 2020) and JSON with JWT (Jones, Bradley, & Sakimura, 2015) serializations of the data model. JSON-LD is the preferred format for many applications including this work. A comparison of JSON-LD over JWT is available in the

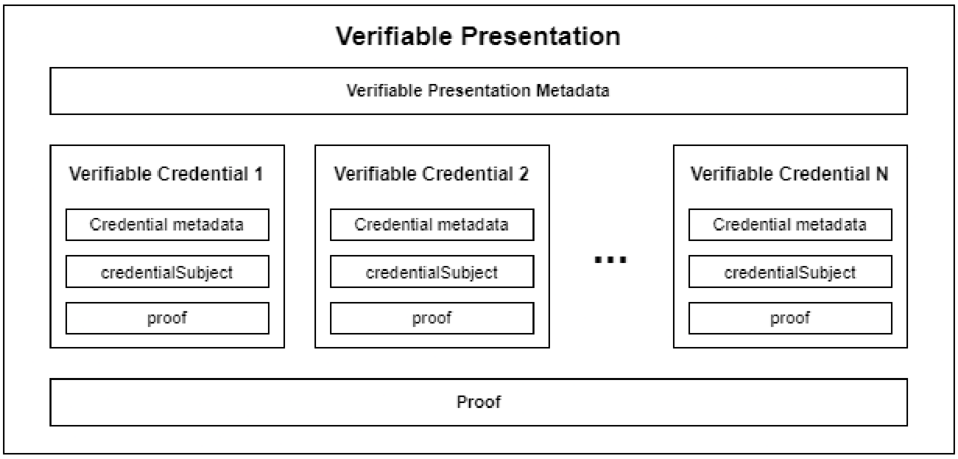


Figure 2.4: Outline of a verifiable presentation

VC implementation guide (D. Chadwick, Longley, Sporny, et al., 2019) and is discussed in K. Young, 2021.

JSON-LD is both an extension to JSON and effectively a Rescource Description Framework (RDF)[1] syntax. The use of JSON-LD accomplishes several things. First, it brings linked data properties with minimal changes to JSON, which is widely used in today's web. Second, it makes possible to model complex real world relationships with a graph model. Third, it enables "permissionless innovation" through extensibility. Anyone can extend the existing vocabularies and numerous cryptographic proof formats and signature suites can be used. This is in line with the "open world assumption" approach, that anyone can assert claims about any subject. It is up to implementers and verifiers to decide based on the real world trust relationships which claims to accept and which entities to trust.

Originally, keys (attributes) in JSON-LD documents are Internationalized Resource Identifier (IRI)s (Dürst & Suignard, 2005), which are similar to Uniform Resource Identifier (URI)s (Berners-Lee, Fielding, & Masinter, 2005) [2]. There's often confusion around URIs, URLs, and URNs. Figure 2.5 and the examples in Listing 2.1 helps understanding the differences. Interested readers may refer to the relevant RFC for further information (Mealling & Denenberg, 2002).

Listing 2.1: URL and URN examples

```
URL: ftp://ftp.is.co.za/rfc/rfc1808.txt
URL: http://www.ietf.org/rfc/rfc2396.txt
```

[1] https://www.w3.org/TR/rdf11-concepts/

[2] The JSON-LD spec uses IRIs but the VC spec only mentions URIs so the two are used interchangeably. This document refers to identifiers as URIs

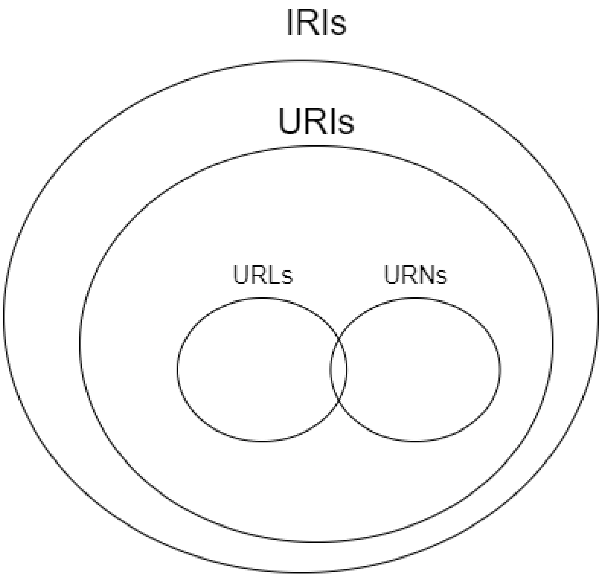


Figure 2.5: Identifiers

```
URL: telnet://192.0.2.16:80/
URL: did:ethr:0xb9c5714089478a327f09197987f16f9e5d936e8a
URN: isbn:0-486-27557-4
URN: uuid:6e8bc430-9c3a-11d9-9669-0800200c9a66
```

The use of identifiers lets machines to unambiguously refer things in the world. For instance the meaning of the property `children` may be obvious for a human-reader depending on the context. If the reader sees the property under a person object, they can infer that it means "a son or a daughter of that person". However, `children` is also used to express hierarchical relationships between things. These semantics need to be stated explicitly for machines to be able to "understand" what these properties stand for and to avoid such ambiguities in machine communication. That's why instead the keys are Internationalized Resource Identifiers. Also to avoid everyone defining their own `child` semantics, shared vocabularies are defined. One popular vocabulary is schema.org. To express "a child of a person", the IRI https://schema.org/children can be given. A JSON-LD document expressing family relationships looks like in Listing 2.2

Listing 2.2: A JSON-LD with full IRIs

```
{
  "@id": "http://doefamily.net/john",
  "http://schema.org/givenName": "John",
  "http://schema.org/familyName": "Doe",
  "http://schema.org/children": {
    "@id": "http://doefamily.net/jane",
    "http://schema.org/givenName": "Jane",
    "http://schema.org/familyName": "Doe"
  }
}
```

However this document is difficult to read. Instead of having to write full IRIs each time, a `@context` can be included in the document that will map terms in the included document to IRIs. Similar to a human communication, this sets the context of the information exchange, thus removing the ambiguity and providing conciseness. A context document for the previous JSON-LD file might be as follows (Listing 2.3).

Listing 2.3: A context file

```
{
  "@context": {
    "firstName": "http://schema.org/firstName",
    "lastName": "http://schema.org/lastName",
    "children": "http://schema.org/children"
}
```

Assuming the context is located at `http://example.com/familyContext`, the previous document becomes more human-readable by embedding the context (Listing 2.4).

Listing 2.4: A context added JSON-LD with shortened terms

```
{
    "@context": "http://example.com/familyContext",
    "@id": "http://doefamily.net/john",
    "givenName": "John",
    "familyName": "Doe",
    "children": {
        "@id": "http://doefamily.net/jane",
        "givenName": "Jane",
        "familyName": "Doe"
    }
}
```

The examples above are JSON-LD documents but they are not verifiable credentials. For a document to be a valid verifiable credential they must have the following properties:

- A `@context` property with the first member https://www.w3.org/2018/credentials/v1.
- A `type`[3] property that includes the type `VerifiableCredential`.
- And the following properties: `credentialSubject, issuer, issuanceDate, proof`

A minimal verifiable credential and a verifiable presentation in JSON-LD format are shown in Listings 2.5 and 2.6.

Listing 2.5: Example verifiable credential (Sporny, Longley, & Chadwick, 2019)

```
{
  "@context": [
    "https://www.w3.org/2018/credentials/v1",
    "https://www.w3.org/2018/credentials/examples/v1"
  ],
  "id": "http://example.gov/credentials/3732",
  "type": ["VerifiableCredential", "UniversityDegreeCredential"],
  "issuer": "https://example.edu",
  "issuanceDate": "2010-01-01T19:73:24Z",
  "credentialSubject": {
    "id": "did:example:ebfeb1f712ebc6f1c276e12ec21",
    "degree": {
      "type": "BachelorDegree",
      "name": "Bachelor of Science and Arts"
    }
  },
  "proof": {
    "type": "RsaSignature2018",
    "created": "2018-06-18T21:19:10Z",
    "proofPurpose": "assertionMethod",
    "verificationMethod": "https://example.com/jdoe/keys/1",
    "jws": "eyJhbGciOiJQUzI1NiIsImI2NCI6ZmFsc2UsImNyaXQiOlsiYjY0Il19
        ↪ DJBMvvFAIC00nSGB6Tn0XKbbF9XrsaJZREWvR2aONYTQQxnyXirtXnlew
        ↪ JMBBn2h9hfcGZrvnC1b6PgWmukzFJ1IiH1dWgnDIS81BH-
```

[3] Alias to `@type`, also `@id` is aliased to `id` in VC

```
        ↪ IxXnPkbuYDeySorc4QU9MJxdVkY5EL4HYbcIfwKj6X4LBQ2_ZHZIu1j
        ↪ dqLcRZqHcsDF5KKylKc1THn5VRWy5WhYg_gBnyWny8E6Qkrze53MR7Ou
        ↪ AmmNJ1m1nN8SxDrG6a08L78J0-
        ↪ Fbas5OjAQz3c17GY8mVuDPOBIOVjMEghBlgl3nOi1ysxbRGhHLEK4s0
        ↪ KKbeRogZdgt1DkQxDFxxn41QWDw_mmMCjs9qxg0zcZzqEJw"
  }
}
```

Listing 2.6: Example verifiable presentation (Sporny, Longley, & Chadwick, 2019)

```
{
  "@context": [
    "https://www.w3.org/2018/credentials/v1",
    "https://www.w3.org/2018/credentials/examples/v1"
  ],
  "type": "VerifiablePresentation",
  "verifiableCredential": [{...}, {...}, {...}],
  "proof": {
    "type": "RsaSignature2018",
    "created": "2018-09-14T21:19:10Z",
    "proofPurpose": "authentication",
    "verificationMethod": "did:example:ebfeb1f712ebc6f1c276e12ec21#keys-1",
    "challenge": "1f44d55f-f161-4938-a659-f8026467f126",
    "domain": "4jt78h47fh47",
    "jws": "eyJhbGciOiJSUzI1NiIsImI2NCI6ZmFsc2UsImNyaXQiOlsiYjY0Il19..
        ↪ kTCYt5XsITJX1CxPCT8yAV-TVIw5WEuts01mq-
        ↪ pQy7UJiN5mgREEMGlv50aqzpqh4Qq_PbChOMqsLfRoPsnsgxD-
        ↪ WUcX16dUOqV0G_zS245-kronKb78cPktb3rk-BuQy72IFLN25DYuNzVBAh 4
        ↪ vGHSrQyHUGlcTwLtjPAnKb78"
  }
}
```

2.2 Public Key Cryptography and JSON-LD

2.2.1 Digital Signatures

At the heart of today's applications and protocols lies the public key cryptography. The encryption scheme is based on a pair of keys: a public key which can be shared publicly or with the verifying party, and a private key which must be kept absolutely secret except its owner. Hence, it is also called asymmetric cryptography. A user can encrypt a message with their private key, and publish the message and their public key. Anyone can then decrypt the encrypted message with the public key which assures this message was encrypted by the owner of the corresponding private key. Also by encrypting messages with the public key, others can ensure only the owner of the corresponding private key can decrypt the message.

This encryption scheme can also be used to create digital signatures. Apart from the key generation there are two main methods in a digital signature scheme. The *sign* function takes a message and a private key as inputs and generates a signature. The *verify* function takes the message, the digital signature, and the public key as inputs and outputs a boolean value `true` if the signature is valid or `false` otherwise. Upon receiving a message and a signature, the receiver, if they know the public key of the sender, can verify it. By verifying the message the receiver can check two things:

1. **Authenticity:** The message is indeed sent by the sender and not someone else
2. **Integrity:** The message they receive is indeed the message sender sent and not tampered with

Thanks to these properties digital signatures can be used to sign documents or software distributions. Public key cryptography and digital signatures create the backbone of the trust and security of today's web through Transport Layer Security (TLS) (Rescorla, 2018) and X.509 digital certificates (Boeyen, Santesson, Polk, et al., 2008).

There are different asymmetric key techniques, but most notable are the RSA (Rivest, Shamir, & Adleman, 1978) and elliptic curve cryptography based systems such as ECDSA (Johnson, Menezes, & Vanstone, 2001) and EdDSA (Josefsson & Liusvaara, 2017). Elliptic curve signature schemes may be based on different elliptic curves with different properties. For instance, Bitcoin uses the ECDSA as the digital signature algorithm and Secp256k1 as its curve, which is the name of the curve used with specific parameters. Together, a signature algorithm and a curve will describe the communicating parties how to encrypt-decrypt or sign-verify messages.

2.2.2 Linked Data Proofs

Digital signatures can be used to ensure the authenticity and the integrity of linked data, in particular of verifiable credentials. For a verifiable credential to be "verifiable", it has to contain a `proof` property which is a digital signature over the contents of the credential. The data model is designed to be proof format agnostic but two implementations are widely used as proof formats and are explained in the specification. One of them is JWT which is also one of the syntaxes. The other one is the Linked Data Proofs (Longley & Sporny, 2021) and used widely with the JSON-LD syntax.

A Linked Data Proof not only tells the verifiers how to verify a document, but also provides additional meta-data such as when the signature is created and what the purpose of the signature is. Again, the vocabulary is included in the document in a `@context` entry and using this shared vocabulary i.e. a shared understanding of how to do a verification and what the signature stands for, the parties of a credential exchange can communicate unambiguously. With that, anyone can create a signature suite and a corresponding vocabulary that can be used in verifiable credentials. The original VC context[4] already contains some cryptographic suites. A security vocabulary is also available under W3C Credentials Community Group[5]. Additional methods can be specified in the Linked Data Cryptographic Suite Registry[6].

A Linked Data Proof has the following properties required (Longley & Sporny, 2021):

- **type:** the name of the cryptographic suite used in the proof such as `RsaSignature2018`, `BbsBlsSignature2020`
- **proofPurpose:** expresses why a proof is created. Avoids the unintended use of the proof such as a verifiable credential proof (`assertionMethod`) being used for authentication (`authentication`)
- **verificationMethod:** expresses how to verify the proof. Usually an identifier resolves to a document containing the keys used for the signature.
- **created:** when the proof is created
- **signature value:** a string representation of the signature created. The key can be `jws`, `proofValue` etc.

It may also contain other values such as a `nonce` or a `domain`.

[4] https://www.w3.org/2018/credentials/v1

[5] https://w3c-ccg.github.io/security-vocab/

[6] https://w3c-ccg.github.io/ld-cryptosuite-registry/

Even though digital signatures ensure the integrity of credentials, they also prevent selective disclosure. A signature is only valid over the whole of the credential and therefore it is not possible to share only some parts of it verifiably. Selective disclosure is a desired property for the minimization of personal data, which is a common principle in privacy regulations such as GDPR (EU, 2016; Langheinrich, 2001).

There are several ways to achieve data minimization (Helmy, 8 May 2020). One way is to contact the issuer each time during the verification and request the required attributes securely. This, called *just in time issuance*, is how information exchange is done through current federated identity providers such as a Google or Facebook log in. Another method is to introduce a trusted third party acting as a *trusted witness*. Publons, in a way acts a trusted witness for the peer reviews and provides review data to parties when needed. Also, it is possible to achieve selective disclosure *cryptographically*.

Using cryptographical methods, there are also several ways selective disclosure may be achieved. An issuer can issue a separate credential for each of the attributes of the combined credential as *atomic credentials*, which allows the holder to present the required attributes (D. W. Chadwick, Laborde, Oglaza, et al., 2019). It is also possible to use *hashed values* in the credential. A holder may then provide the pre-images of the hashed values which they want to disclose to the verifier without having to share all the fields (R. Mukta, J. Martens, H. -y. Paik, et al., 2020, p. 961). Similarly, instead of storing the hash of the credential, a *Merkle tree* of fields can be stored. A holder can present values of the desired attributes and the required hashes in the Merkle tree to enable verification of the disclosed attributes (Hitchens, 2018). Finally, there exist digital signatures that support *Zero-Knowledge Proofs (zk-proofs)* and the selective disclosure of the attributes such as Camenish-Lysyanskaya (Camenisch & Lysyanskaya, 2002), and BBS+ signatures (Boneh & Boyen, 2004; Camenisch, Drijvers, & Lehmann, 2016; Lodder & Looker, 2020).

2.2.3 Zero-Knowledge Proofs

Zero-knowledge proofs of knowledge are protocols in cryptography where a *prover* can cryptographically prove to a *verifier* the validity of a statement without sharing any other information than the fact that the statement is true. The field recently received more attention with the implementation of the privacy-preserving digital currency Zcash (E. Ben Sasson, A. Chiesa, C. Garman, et al., 2016). Even though commonly referred as zero-knowledge proofs, it is useful to distinguish between *proofs* and *proofs of knowledge*. A proof is sufficient evidence for the truth of a proposition such as a proof for the statement that there exists a three coloring for a specific graph. A proof of knowledge is a proof for the knowledge of a piece of information such as a proof to the statement that one knows a three coloring for a specific graph (Green, 2017).

Properties of zero-knowledge proofs are as follows (Groth, 2010):

- **Completeness:** If the statement is true, the verifier will be convinced by the proof the prover presents that the statement is true
- **Soundness:** If the statement is false, a malicious prover can not convince the verifier that it is true.
- **Zero-Knowledge:** If the statement is true, a malicious verifier does not learn anything else than the fact that the statement is true.

The first two properties are also requirements for interactive proofs. The work of Goldwasser, Micali, and Rackoff, 1985 has first introduced the third property of Zero-Knowledge. A proof in a zero-knowledge proof system is not deterministic but a probabilistic proof. Through many rounds it is possible to decrease the error to practically negligible values. Goldreich, Micali, and Wigderson, 1991 also show that with the assumption of an unbreakable encryption, it is possible to create a zero-knowledge proof for the graph coloring problem. This is significant since the graph coloring problem is NP-complete and every NP problem can be reduced to an NP-complete problem in polynomial time, meaning every problem in NP has a zero-knowledge proof.

These initial zero-knowledge proofs are also interactive, that is the prover and the verifier need to exchange information on each round. Each time a proof is needed to be made, the prover and the verifier need to be online and interact in multiple rounds, which makes the usability of the protocol difficult. Also, since the soundness of the proof relies on the randomness of the challenges of the verifier on each round, a third-party cannot be convinced by such a proof. By looking at the protocol transcript and the proof, they can not be assured if this randomness holds. Blum, Feldman, and Micali, 1988 have shown that with a common reference string shared by the prover and the verifier, it is possible to create non-interactive zero-knowledge proofs. The common reference string need not be private, which makes non-interactive zero-knowledge proofs more practical than interactive ones.

2.3 Decentralized Identifiers

Decentralized Identifier (DID)s (Reed, Sporny, Longley, et al., 2021) are a new type of globally unique identifiers that do not depend on centralized identity providers or registries, and give their users full control of their identity. DIDs follow the URI syntax with a `did:` scheme followed by a method and the method specific identifier. Some examples of DIDs are given in Listing 2.7.

Listing 2.7: Decentralized Identifier examples

```
did:example:123456789abcdefghi
did:example:123456789abcdefghi#key-1
did:example:123456789abcdefghi?versionTime=2021-05-10T17:00:00Z
// Ethereum
did:ethr:0xb9c5714089478a327f09197987f16f9e5d936e8a
// Sovrin
did:sov:mnjkl98uipsndg2hdjdjuf7
// Public-key embedded DID
did:key:z6MkpTHR8VNsBxYAAWHut2Geadd9jSwuBV8xRoAnwWsdvktH
// Web
did:web:example.com
```

Each DID resolves to a DID document, similar to how `http://www.example.com` resolves to an HTML file. Different methods have different resolvers and may have their own internal way of creating method specific identifiers. A DID document describes the meta-data associated with the object it identifies in a JSON-LD format. This may include the public keys associated, the controller of the document, the services and the service endpoints available for the described object etc. The DID `did:example:123456789abcdefghi` may resolve to the following document in Listing 2.8 which describes two public keys assoicated with it for verification purposes, and one for authentication. It also expresses that this object is controlled by the DID `did:example:bcehfew7h32f32h7af3`, and a service associated with it. This may for instance be an identifier for an IoT device with an `EncryptedDataVault` owned by a user identified with `did:example:bcehfew7h32f32h7af3`.

Listing 2.8: Example Decentralized Identifier document (Reed, Sporny, Longley, et al., 2021)

```
{
  "@context": [
    "https://www.w3.org/ns/did/v1",
    "https://w3id.org/security/suites/ed25519-2020/v1"
  ]
  "id": "did:example:123456789abcdefghi",
  "controller": "did:example:bcehfew7h32f32h7af3",
  "verificationMethod": [{
      "id": "did:example:123456789abcdefghi#key-1",
      "type": "Ed25519VerificationKey2020",
      "controller": "did:example:123456789abcdefghi",
      "publicKeyMultibase": "zH3C2AVvLMv6gmMNam3uVAjZpfkcJCwDwnZn6z3wXmqPV"
    },
    {
      "id": "did:example:123456789abcdefghi#key-2",
      "type": "Ed25519VerificationKey2020",
      "controller": "did:example:123456789abcdefghi",
      "publicKeyMultibase": "Zpfs4h2fkcJCwDNam3uVAjZpwnZn6z3wXmo91LvLMv6A"
    }
  ],
  "authentication": [
    "#key-1"
  ],
  "service": [{
    "id": "did:example:123456789abcdefghi#vault",
    "type": "EncryptedDataVault",
    "serviceEndpoint": "https://edv.example.com/"
  }]
}
```

DIDs and VCs are both part of the Self-Sovereign Identity (SSI) ecosystem. Still, both specifications are separate and do not depend on each other. Since DIDs are URIs, they can be used in the fields that are required to be URIs in verifiable credentials. This includes `id` fields, `issuer`, `verificationMethod`. Using DIDs in `issuer` and `verificationMethod` leverages the public keys associated with DIDs and the verification can be done using the keys associated.

3 Design & Implementation

The goal of this work is to design a system that will allow the verification of closed peer reviews without a trusted third party. The new artifact should improve upon the existing ones, which are the current peer review showcase platforms. Based on the problems identified, the requirements of such a system is defined in the following section. Taking these requirements and available technologies into account, a design of a system will be communicated. Additionally, the implemented proof of concept prototype will be demonstrated.

3.1 Requirements

As stated in the problem statement, current lack of recognition of peer reviews stems from the public unavailability of the closed peer reviews. Each individual party presented with the peer reviews of a researcher needs to explicitly contact each journal if they want to verify the peer reviews. This is clearly infeasible in a public setting: if a researcher has their peer reviews stated in a public profile, e.g. on their website, each party consuming this data has to contact the journals. This is not the case for other scholarly works such as manuscripts. Therefore, it should be easy to check if the peer review is authentic, that is, the peer reviews are **verifiable**.

Currently, there are platforms for aggregating and showcasing peer reviews. The process of adding peer reviews to these platforms include automatic methods such as integrations with journals. Users can also add reviews manually such as by sending the review receipt emails or by filling out the review information on the platform. These will get checked by the platform and then the peer review will be "verified". However, it is not possible to trace how the review is verified and it is at the platforms discretion to decide what constitutes a verified review and what is not. There are researchers on these platforms that have over 1000 verified reviews per year on their profile. Questions about the validity of this data has been raised (Teixeira da Silva, 2017, 2020; Teixeira da Silva & Al-Khatib, 2019). Following the open science principles it is important to provide provenance on data and **transparency** on how the verification is done.

It is outlined in previous sections, how the review showcasing platforms aggregate review data by acting as trusted third-parties. They become the sources of peer review contributions of a researcher and decide what is a "verified" review. The data stored by the platforms is different than what is available to public, which enables potentially putting the data behind a paywall or charging its users. Therefore, **open data** is another requirement of the system. In parallel, by having a system design based on **open standards**, vendor lock-in can be avoided. This lets anybody provide review showcasing services and users will have the freedom to choose which service they want to use. Also, the platforms' ability to hold onto the peer review data is provided by their position as the trusted third-parties. Instead, it is desirable to create direct trust between the parties. The designed system should facilitate **direct trust** between the stakeholders.

A peer review has various metadata associated. The necessary data to be presented may be different in each context. For a review author it is useful to be able present different data associated with the review without breaking the verifiability of the review. For instance, the contents and the date of a closed review may not be shared on a public profile, but a review author might want to share these in a more private setting such as in a job or grant application. In both cases, the reviewer should be able to **selectively disclose** which attributes they want to share.

Peer review practices vary a lot between fields, even from journal to journal within the same field. Hence, the required system should be **compatible** with the different practices and different data resulting from these processes. The system should enable the creation of different data schemas, but at the same time avoid ambiguity and let stakeholders communicate what this data means.

Here the requirements are listed together once again.

- RQ1: Verifiability
- RQ2: Transparency
- RQ3: Open Data
- RQ4: Open Standards
- RQ5: Direct Trust
- RQ6: Selective Disclosure
- RQ7: Compatibility

3.2 Design

3.2.1 Overview

As the basis the W3C's Verifiable Credentials specification (Sporny, Longley, & Chadwick, 2019) is chosen. The specification inherently satisfies some of the requirements of the system. It is verifiable (RQ1), based on open standards (RQ4), and built with an open world assumption, that is, anyone can extend the existing vocabularies and can issue credentials (RQ7). Also, there exist open source VC libraries that can be used in the implementation.

The designed system has two main components:

1. **Journal X:** A hypothetical journal that issues peer review credentials
2. **Veriview:** An open source peer review showcase platform that supports peer review VCs

In a typical peer review process, a researcher receives an invitation to do a peer review from the editor of the journal. Here, upon receiving an invitation from Journal X, the reviewer accepts it and submits the review of the manuscript to Journal X. Then she can request the proof of their work as a peer review verifiable credential. Journal X prepares the credential and issues it by signing the document. The review author can use this credential to prove their authorship. A peer review showcasing platform called Veriview is also conceived, where review authors can build their "peer review resume". According to the privacy policy of the review, they can decide which information about the review to share publicly. For instance, a blinded review typically can not be shared with identifiable information such as the manuscript, the content, the title etc. The reviewer is able to choose which information to share on their public profile accordingly. An overview of the interactions of the typical use case on the system are depicted below in Figure 3.1

In practice, there supposed to be many journals and Journal X is one example out of numerous journals. Also Veriview is not a single platform but there may be many showcasing platforms that researchers can choose to build their profiles at. Having a system based on open standards (RQ4) allows anyone to create a platform similar to Veriview and this would avoid vendor lock-in.

Additionally assumed is a "Review Data Consumer", a party which is interested in the peer review data of a reviewer. In real world these might be employers, universities, research institutions, or other researchers. This can also be other applications that want to make use of the peer review contributions of researchers. For example, a peer review matching application that would suggest potential reviewers to editors or platforms aiming to incentivize reviewers

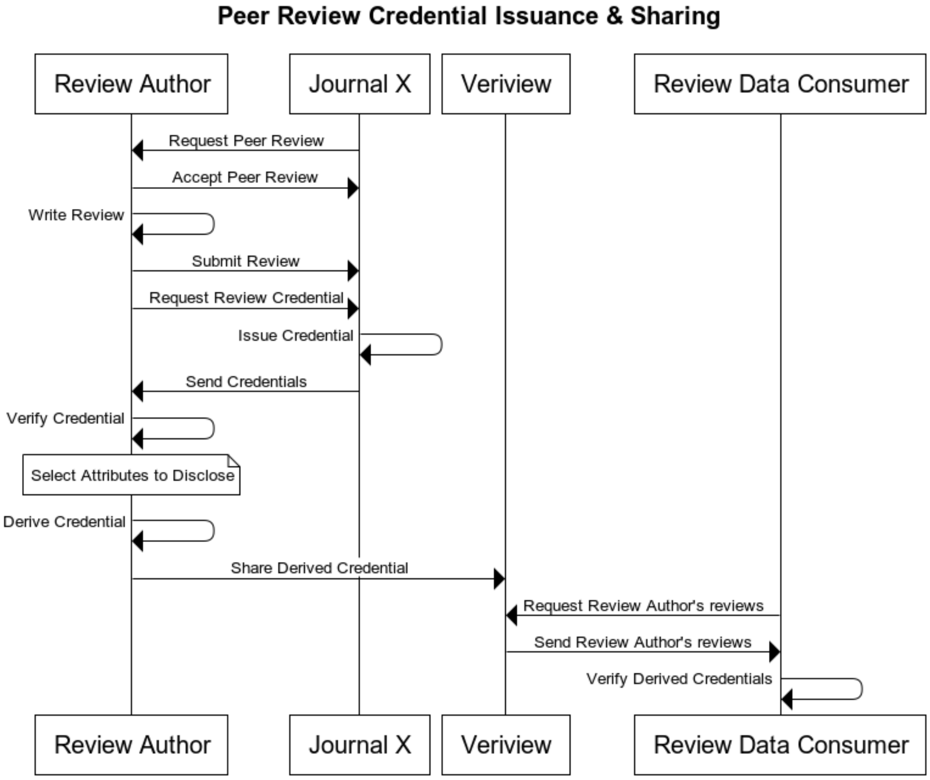


Figure 3.1: Overview of peer review credential issuance and sharing process

(Jan, Third, Ibanez, et al., 2018; Tenorio-Fornés, Jacynycz, Llop-Vila, et al., 2019; Trovò & Massari, 2021) with rewards can make use of this open data (RQ3). Any party that is interested in the peer reviews of a researcher, and their authenticity, might be a consumer.

The use case depicted in Figure 3.1 assumes the reviews are shared publicly and are not open reviews. Open reviews would not require additional derivation as all of the review data can be shared publicly and they are verifiable themselves where they are published. Since Veriview is a platform to share blinded peer reviews publicly, the review author will choose which attributes they want to and are able to share, and derive a credential containing the selected attributes and a zero-knowledge proof which can be shared in Veriview.

In a private setting or for an open review this additional derivation step is not required. For instance, if the researcher wants to include their review in a grant application, they might want to share the reviewed manuscript and the contents of the review. If the manuscript is in the scientific field the researcher wants to show competence in, being able to verifiably show that they were invited and done a review in this field would demonstrate the researcher's competence. Also, other factors such as the journal's reputation provide additional information. In this case Veriview is not required and the interactions are as in Figure 3.2.

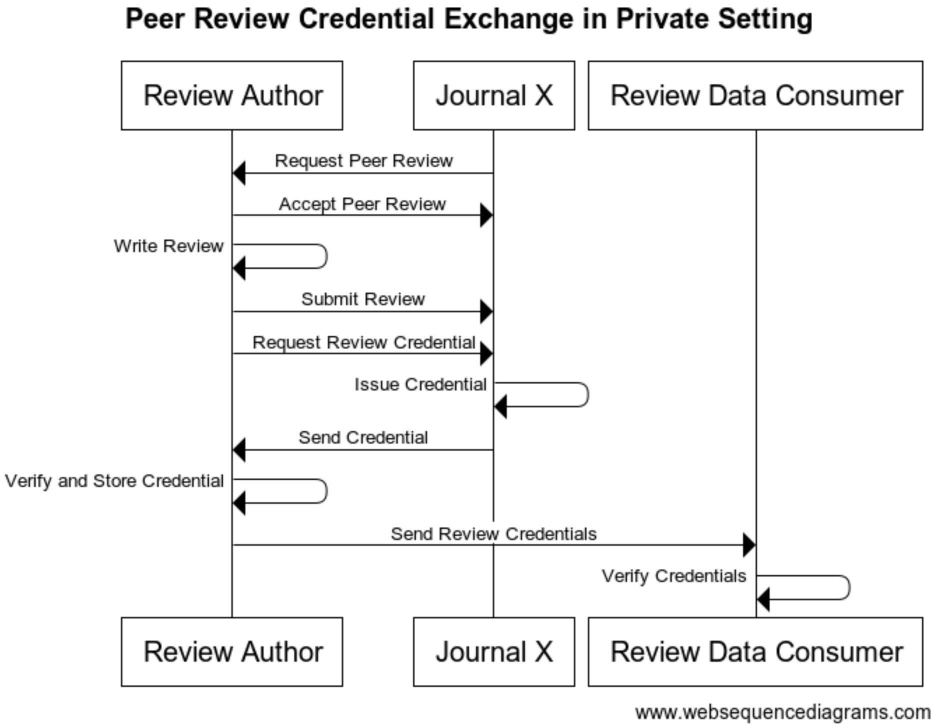


Figure 3.2: Peer review credential exchange in a private setting

3.2.2 Peer Review Credential

The Peer Review Credential is a document issued by a journal that a peer review has been done for this journal. The document contains the review content and the metadata associated such as the date, title, author etc. An example credential is given below in Listing 3.1

Listing 3.1: Example Peer Review Credential

```
{
  "@context": [
    "https://www.w3.org/2018/credentials/v1",
    "https://raw.githubusercontent.com/kuzdogan/peer-review-verifiable-
        ↪ credentials-thesis/main/code/PeerReview.json",
    "https://w3id.org/security/bbs/v1"
  ],
  "type": [
    "PeerReviewCredential",
    "VerifiableCredential"
  ],
  "id": "https://journalx.com/reviews/60afb3a10c601a002c8a43fe/credential",
  "description": "A Verifiable Credential representing a peer review that is
      ↪ done for a scholarly article.",
  "name": "Peer Review Credential version 0.1",
  "issuanceDate": "2021-05-27T15:33:28.743Z",
  "issuer": "did:web:journalx.com",
  "credentialSubject": {
    "id": "https://journalx.com/reviews/60afb3a10c601a002c8a43fe",
    "type": "PeerReview",
    "competingInterestStatement": "",
    "reviewDate": "2021-05-27T14:58:41.746Z",
    "title": "Review: Australian state influenza notifications and school
        ↪ holiday closures in 2019",
    "content": "Summary: Australias influenza season does not typically
        ↪ coincide with school holidays. ... The observed and predicted plots
        ↪ in Appendix 3 appear to show 3 different segments fit for each of
        ↪ these periods, but it is unclear what change is reported in Table
        ↪ 1.",
    "recommendation": "Accept",
    "journal": {
      "id": "https://journalx.com/",
      "issn": "2046-1402",
      "name": "International Journal of X"
    },
    "manuscript": {
      "id": "https://doi.org/10.1000/182",
      "title": "Australian state influenza notifications and school holiday
          ↪ closures in 2019",
      "abstract": "Background: The impact of school holidays on influenza rates
          ↪  has been sparsely documented in Australia. In 2019, the...these
          ↪ results have important public health implications. Closure or
          ↪ extension of holiday periods could be an emergency option for state
          ↪  governments."
    },
    "author": {
      "id": "did:key:z6MkpTHR8VNsBxYAAWHut2Geadd9jSwuBV8xRoAnwWsdvktH",
      "type": "PeerReviewAuthor",
      "email": "john@uni-example.edu",
      "familyName": "Doe",
      "givenName": "John"
    }
  },
  "proof": {
    "type": "BbsBlsSignature2020",
    "created": "2021-05-27T15:33:28Z",
    "nonce": "PvEw7iQVMcSiXrzQFg2+
        ↪ Y44aD4I0W0wKJyVWeUPtL1oGoY37ukNP81VipIl8N1LoIAY=",
    "proofPurpose": "assertionMethod",
    "proofValue": "r1jtn/bxSof/0
        ↪ UOAlnro1bm217GIhENtezDWMKxubTQvybwSD62LoEkQfFD4PkhSHJjSv 888
        ↪ GciT5vpG5TareYENbLXa4W91/S2CTVwvwlYgt/moCC8/
        ↪ OC63wG2hskjQiOJcZ3wZ4Bki8gZ2vVPKvQ==",
    "verificationMethod": "did:web:journalx.com#credentialsKey"
  }
}
```

The credential in this design follows the JSON-LD syntax. JSON-LD is the predominantly used format in the VC specification. It is also an open standard under W3C (Sporny, Longley, Kellogg, et al., 2020) (RQ4) and many of the VC libraries available are JSON-LD based. JSON-LDs with Linked Proofs supports Zero-Knowledge Proof formats and JSON-LDs require canonicalization, which allows flexibility in the order of the attributes. This becomes useful for instance when transferring the credential from the journal to the author, the journal doesn't have to worry about the order of the attributes when they issue the credential. Also, being fully compatible with JSON, the format easily integrates with existing web frameworks.

The credential is designed to represent the review as the subject. Under `credentialSubject` the data related to review is contained, including the `author` field which represents the author of the review. An alternative representation could be to issue a "review authorship" credential which would contain the author as the credential subject and an `authoredReview` field containing the review data. Both are valid expressions of the same relationships, but here it is chosen to represent the review itself as the system is for "peer review credentials" and a peer review credential implies the review itself is the credential being issued. In the other case, it is needed to express the credential as a "peer review authorship credential" explicitly and this might create confusion.

Context

`@context` defines the vocabularies used in the document. The first URL refers to the VC context and it is required to be included in all verifiable credentials according to the specification. The second context contains the vocabulary specific for peer reviews which is defined for this system. Finally, `https://w3id.org/security/bbs/v1` provides the vocabulary for the `BbsBlsSignature` signature suite since it is not included in the default `https://www.w3.org/2018/credentials/v1` context. The context used in this document is given in Listing 3.2

Listing 3.2: Peer Review Vocabulary

```
{
  "@context": {
    "@version": 1.1,
    "schema": "http://schema.org/",
    "PeerReviewCredential": {
      "@id": "https://raw.githubusercontent.com/kuzdogan/peer-review-verifiable-
        ↪ credentials-thesis/main/code/PeerReview.json#PeerReviewCredential",
      "@context": {
        "@version": 1.1,
        "id": "@id",
        "type": "@type",
        "description": "schema:description",
        "name": "schema:name"
      }
    },
    "PeerReview": {
      "@id": "https://raw.githubusercontent.com/kuzdogan/peer-review-verifiable-credentials-thesis/main/code/PeerReview.json#PeerReview",
      "@context": {
        "@version": 1.1,
        "id": "@id",
        "type": "@type",
        "title": "schema:headline",
        "content": "schema:text",
        "reviewDate": "schema:dateCreated",
        "competingInterestStatement": "schema:Text",
        "recommendation": "schema:Recommendation",
        "journal": {
        "@id": "https://raw.githubusercontent.com/kuzdogan/peer-review-verifiable-credentials-thesis/main/code/PeerReview.json#journal",
        "@context": {
          "@version": 1.1,
          "id": "@id",
          "type": "@type",
          "name": "schema:name",
          "issn": "schema:issn"
        }
        },
        "manuscript": {
        "@id": "https://raw.githubusercontent.com/kuzdogan/peer-review-verifiable-credentials-thesis/main/code/PeerReview.json#manuscript",
          "@context": {
            "@version": 1.1,
            "id": "@id",
            "type": "@type",
            "title": "schema:headline",
            "abstract": "schema:abstract"
          }
        },
        "author": "https://raw.githubusercontent.com/kuzdogan/peer-review-
            ↪ verifiable-credentials-thesis/main/code/PeerReview.json#author"
      }
    },
    "PeerReviewAuthor": {
      "@id": "https://raw.githubusercontent.com/kuzdogan/peer-review-verifiable-
          ↪ credentials-thesis/main/code/PeerReview.json#PeerReviewAuthor",
      "@context": {
        "@version": 1.1,
        "id": "@id",
        "type": "@type",
        "givenName": "schema:givenName",
        "familyName": "schema:familyName",
        "institution": "schema:Organization",
        "email": "schema:email"
      }
    }
  }
}
```

The vocabulary document itself is a context that defines three different contexts, namely `PeerReviewCredential`, `PeerReview`, and `PeerReviewAuthor`. These contexts can be included in the corresponding objects in the credential by adding to the `type` field in the JSON-LD credential document. The `@version` term defines the JSON-LD version of the definition. This will explicitly tell the JSON-LD processor to use the version 1.1 processing mode. It is not a requirement to set the version explicitly but this practice avoids potentially processing the document with the older JSON-LD processors.

In the vocabulary, terms from schema.org was used when there exist a clearly overlapping term in the schema.org ontology, such as the ISSN field or the title field which corresponds to schema.org/headline. In other cases, self-referring definitions are made, which refer to themselves in the `@id` field, as in the case with the `author` or `journal` fields. There exists a term for `author` in schema.org but it is preferred for the schema to be explicit and to be included in credential document through adding the `PeerReviewAuthor` in the `type` field. Similarly, an explicit definition of `journal` is preferred over the general `schema.org/Periodical` term. Also, by defining the term `"schema": "http://schema.org/"` it is made possible to map the URL paths to the schema.org. As an example, this allows `schema:name` to be expanded into `http://schema.org/name` when processed.

The previous version of the defined peer review vocabulary included `@protected: true` attributes in `@context`'s, which prevents overriding attributes by new definitions. Even though this adds extra protection to term definitions, it disallows the extension on the definitions. It is removed to enable extensibility. The peer review process varies a lot at each publisher or journal, and issuers can adopt the vocabularies according to their needs. The vocabulary assumes a basic credential model with few attributes associated with a peer review. Thanks to the extensibility of JSON-LD vocabularies, it possible to extend the vocabulary itself, or include other vocabularies in the document. For instance, if the peer review process of a journal has a statistical soundness check, this can be represented as a `statisticallySound` field defined in another vocabulary and included in the credential context. This enables the compatibility of the system (RQ7) with different peer review processes. Ideally, these vocabularies will be defined with different stakeholders of the peer review ecosystem coming together, that they will be widely accepted and used.

Signatures

Expressed by the `BbsBlsSignatureProof2020` type in the `proof` field, BBS+ signatures with a BLS12-381 curve is the chosen signature suite. BBS+ signatures is the preferred signature scheme while BLS12-381 is the curve used for generating the keys. BBS+ signatures can be used with any pairing friendly curve (Sakemi, Kobayashi, Saito, & Wahby, 2020), but since the existing Linked Data Proof signature suite (Looker & Steele, 2021) and the implementations[1] are based on BLS12-381 curves, the same curve was adopted. This signature suite allows zero-knowledge selective disclosure of attributes (RQ6) with more efficient size and execution times (Lodder, 2019) compared to the existing ones such as CL signatures.

With BBS+ signatures it is possible to sign multiple messages. The signature scheme provides a *sign* and a $verify$ verify function that are also found in other digital signature

[1] https://github.com/mattrglobal/bbs-signatures-spec

schemes. The signature is not over the whole message and the size of the signature is variable with the number of messages hidden. For an array of messages $m[0], m[1], ..., m[n]$, a public key *privk*, a private (secret) key *pubk* the below functions are provided.

$$signature = sign((m[0], m[1], ..., m[n]), pubk, privk)$$

$$result = verify((m[0], m[1], ..., m[n]), signature, pubk)$$

Where result is a boolean value representing the validity of the signature. Additionally, the BBS+ signatures allows derivation of a *proof* of knowledge of the original signature and the verification of the proof. A party who knows the messages, the public key, and the signature over all of the messages can take a subset of the messages and create a zero-knowledge proof as follows:

$$proof = derive((m[3], m5], ..., m[n-1]), signature, pubk)$$

Which can be verified with:

$$result = verifyProof((m[3], m[5], ..., m[n-1]), proof, pubk)$$

With the BLS12-381 curve the element sizes are as follows (MATTR, 2021):

Element	Size
$privk$	32 bytes
$pubk$	96 bytes
$signature$	112 bytes
$proof$	368 + (hidden message count) x 32 bytes

Decentralized Identifiers

The VC specification describes several attributes as identifiers (i.e. URIs). Apart from uniquely identifying the described object, these fields may also be used for authentication. In the case of `issuer`, the value of the attribute is recommended to resolve to a document that can be used to verify the credential. The document would contain the public key information of the signer key, and other meta-data related to the issuer. Similarly, a DID in the `author` field can be used for verification in a credential exchange. The holder of the credential (author) can wrap the credential or multiple credentials in a verifiable presentation to ensure it is being sent from the intended holder.

In this system, the issuer field is a DID of the journal. It is required for the verifiability of the peer reviews to have this identifier field resolve to a document with a public key (RQ1). Although it is possible to use an HTTP URL that resolve to a document containing public keys, DIDs are preferred since it provides a standard document format that can be used for verification, and for their close relationship with VCs in the SSI ecosystem.

Using a DLT based DID method would provide the document a high availability, tamper-proofness, and won't require to contact the issuer at each verification. An example would be `did:sov:mnjkl98uipsndg2hdjdjuf7` which represents a DID that can be resolved with the Sovrin blockchain method. However, it would be necessary to bind this DID with the real world identity of the journal. By looking at the identifier `did:sov:mnjkl98uipsndg2hdjdjuf7`, a third-party is not able to infer that this is the identity associated with Journal X. In that case, the identifier `did:sov:mnjkl98uipsndg2hdjdjuf7` needs to be announced as belonging to Journal X in different channels. This may be in a non-digital communication or by announcing the identifiers on the journal website. An alternative in the DID space is to create accreditation registries. Similar to accreditation in real world, a third party or a joint organization can keep a registry of vouched identities, and can provide the necessary trust. However, this may lead to centralization and is similar to the centralization vs. decentralization dichotomy in the web PKI systems (Perlman, 1999).

Here, `did:web`[2] is the preferred DID method used for the `issuer` field. Compared to a DLT method this would require the server of the DID document to be highly available and the controller of the server may change the file without others noticing. The advantage is that this method makes use of the identity provided by the journal's host address (e.g. https://www.journalx.com) and its X.509 certificate (Barclay, Radha, Preece, et al., 2020, p. 4). The website of journals are usually known and can serve as a valid identifier thanks to the existing public key infrastructure. It is also human readable, and there exist implementations of `did:web` resolvers. To have a DID document resolved from its identifier, a host can serve it under the well-known path (Hammer-Lahav & Nottingham, 2010) `https://<HOST-NAME>/.well-known/did.json`.

Also, as the `author` identifier a DID can be used. The example credential in Listing 3.1 contains a `did:key` DID (Longley, Zagidulin, & Sporny, 2021) that has its identifier as the Multibase format (Benet & Sporny, 2021) of its public key and simply expands to a document containing the same public key used for different verification methods. It is also possible to use different DIDs such as a DLT based one. By resolving the DID to a DID document, the authentication of the holder can be done. In our case, it will enable authenticating that the party presenting the credentials (holder) are actually the author stated in the `author` field.

[2] https://w3c-ccg.github.io/did-method-web/

This can be done by wrapping the credentials in a verifiable presentation. In theory any identifier field can be a DID but this comes at the cost and effort of the management of the identity and the keys.

Listing 3.3: DID document corresponding to the DID `did:key:z6MkpTHR8VNsBxYAAWHut2Geadd9jSwuBV8xRoAnwWsdvktH` (Longley, Zagidulin, & Sporny, 2021)

```
{
  "@context": "https://w3id.org/did/v1",
  "id": "did:key:z6MkpTHR8VNsBxYAAWHut2Geadd9jSwuBV8xRoAnwWsdvktH",
  "publicKey": [{
    "id": "did:key:z6MkpTHR8VNsBxYAAWHut2Geadd9jSwuBV8xRoAnwWsdvktH#
        ↪ z6MkpTHR8VNsBxYAAWHut2Geadd9jSwuBV8xRoAnwWsdvktH",
    "type": "Ed25519VerificationKey2018",
    "controller": "did:key:z6MkpTHR8VNsBxYAAWHut2Geadd9jSwuBV8xRoAnwWsdvktH",
    "publicKeyBase58": "B12NYF8RrR3h41TDCTJojY59usg3mbtbjnFs7Eud1Y6u"
  }],
  "authentication": [ "did:key:z6MkpTHR8VNsBxYAAWHut2Geadd9jSwuBV8xRoAnwWsdvktH
      ↪ #z6MkpTHR8VNsBxYAAWHut2Geadd9jSwuBV8xRoAnwWsdvktH" ],
  "assertionMethod": [ "did:key:
      ↪ z6MkpTHR8VNsBxYAAWHut2Geadd9jSwuBV8xRoAnwWsdvktH#
      ↪ z6MkpTHR8VNsBxYAAWHut2Geadd9jSwuBV8xRoAnwWsdvktH" ],
  "capabilityDelegation": [ "did:key:
      ↪ z6MkpTHR8VNsBxYAAWHut2Geadd9jSwuBV8xRoAnwWsdvktH#
      ↪ z6MkpTHR8VNsBxYAAWHut2Geadd9jSwuBV8xRoAnwWsdvktH" ],
  "capabilityInvocation": [ "did:key:
      ↪ z6MkpTHR8VNsBxYAAWHut2Geadd9jSwuBV8xRoAnwWsdvktH#
      ↪ z6MkpTHR8VNsBxYAAWHut2Geadd9jSwuBV8xRoAnwWsdvktH" ],
  "keyAgreement": [{
    "id": "did:key:z6MkpTHR8VNsBxYAAWHut2Geadd9jSwuBV8xRoAnwWsdvktH#
        ↪ zBzoR5sqFgi6q3iFia8JPNfENCpi7RNSTKF7XNXX96SBY4",
    "type": "X25519KeyAgreementKey2019",
    "controller": "did:key:z6MkpTHR8VNsBxYAAWHut2Geadd9jSwuBV8xRoAnwWsdvktH",
    "publicKeyBase58": "JhNWeSVLMYccCk7iopQW4guaSJTojqpMEELgSLhKwRr"
  }]
}
```

Peer Review Credential Issuance & Verification

Once a reviewer accepts and submits their review, they can request a peer review credential from the journal. At this step, the journal may decide not to issue the credential, if, for instance, the decision to publish the manuscript or not is not given, or if the paper is not published yet. In an implementation, the issuance process can be handled by a module or a plugin of the existing journal management systems. There exist many journal management system handling the publication process, including the peer review. These systems have their databases and sometimes APIs working. A working peer review credential module would only need to access this data of each user, pack them together in proper format, sign, and issue the credential.

While preparing the credential document, a journal needs to pay attention to the identifiers used. As stated, the system requires an identifier that will enable the verification of the credential. Accordingly a `did:web` based DID for the journal identifier can be used. If that is the case, the journal needs to publish the DID document under the well-known URL. The `author` identifier is particularly interesting as there are several options available: A Decentralized Identifier (DID), a centralized global identifier such as an ORCID, or an internal identifier of the journal issuing the credential.

In a typical VC flow there are several steps of verification outlined on Table 3.1. Once the reviewer receives the credentials from the journal, they or their wallet will verify the received review credential. This process only requires the **credential verification** step to be completed as the credential exchange is between the issuer and the holder. A wallet is a software for the secure storage and exchange of credentials. This usually comes in the form of a mobile application. The VC specification does not define a protocol for the credential exchange, but the credential transfer should also take place through a secure channel between the holder and the issuer such as DIDComm[3]. The wallet also negotiates and establishes this secure channel with the issuer. A holder may have more than one credentials in a wallet, and they can pack these credentials together to form a verifiable presentation. This signed form of presentation also ensures that the credentials are packed and being presented by the holder. Once received the reviewer verifies and stores these credentials in their wallet.

Upon storing the credential, the holder can share these credentials. The `author` identifier used in the credential will affect which verification steps will be available. A DID that resolves to a DID document would enable authenticating the holder in a credential exchange by wrapping the credentials into a verifiable presentation. In our case this exchange either takes place in a private setting e.g. between a reviewer and a review data consumer, or when

[3] https://identity.foundation/didcomm-messaging/spec/

Table 3.1: Verification steps in a generic VC credential exchange

Steps	Checks	Methods
Presenter authentication	Credentials are being presented by their intended holder.	Check if the identity of the creator of the presentation match with the identities of the intended holder of the credentials.
Holder check	The holder is already known and trusted.	Check if the holder identifier is whitelisted.
Presentation verification	The presentation is created by the holder and not someone else.	Validating the signature of the presentation and the presentation document against an associated public key found in the document when the holder identifier is resolved
Issuer check	The issuer is already known and trusted.	Check if the issuer identifier is whitelisted, and their claims in this context are trusted.
Credential verification	The credential is issued by the stated issuer. The credential has not been tampered with.	Validating the signature of the credential and the credential document against an associated public key found in the document when the issuer identifier is resolved
Revocation check	The credential has not been revoked.	Check the credential in the credential revocation registry.

sharing the derived credentials to Veriview publicly.

Verification of credentials in the private case will have the following steps:

- **Presenter authentication:** All `author` DIDs of review credentials match the DID in the `verificationMethod` of the wrapper presentation's `proof`.
- **Holder check**: Make sure the presenter DID actually belongs to the researcher that review consumer wants to verify. This can be done through an external attestation, for instance a verifiable credential from the research institute of the reviewer that they work there, or by the review consumer's own means such as an email-password authentication.
- **Presentation verification:** The created presentation was signed by a key associated with the DID in the `verificationMethod`.

- **Issuer check:** Check if the review consumer knows and trusts the issuers of the review credentials i.e. the `did:web` of the journals.
- **Credential verification:** Verify individual credentials that they are indeed signed by the associated key of the issuer DID.

Note that the design does not require a revocation check as for reviews this is not a common use case, unlike manuscripts. However, it is still a required step for most VC verifications.

In the public case i.e. on Veriview, normally each credential represents a review contribution, and the credentials would be displayed on a researcher's public profile. If the platform is to verify the presentation and unpack it into credentials and display them, this would eliminate the holder validation and authentication steps and place Veriview into a trusted third-party position. Therefore, not only the credentials but also the presentations need to be shared alongside the credentials. This will make sure that the information regarding authorship of the presentation will not be lost and can be verified by anyone publicly.

Verification on Veriview is similar to the private case, but the verification starts from a single review as the reviews of a researcher are shown on their profile. The steps are as follows:

- **Credential verification:** Check if the review credential is signed by the associated public key of the issuer DID.
- **Presenter authentication:** Find the verifiable presentation where the review credential is embedded. Verify that the author DID in the credential match the DID in the `verificationMethod` of the wrapper presentation's `proof`.
- **Presentation verification:** Check that the presentation was signed by a key associated with the DID in the presentation `verificationMethod`.

The steps above can be completed by the Veriview application and the results of the verification can be communicated to the user on the application interface. This requires a degree of trust to the Veriview application, but by open sourcing (RQ2) the application and allowing users to download the credentials and presentations, and verifying themselves, the required trust can be minimized.

The **holder check** step can be done by the Veriview by associating the DID with the Veriview user account. The association can be done by sending a challenge to the user and asking them to sign the challenge with an associated public key. The **issuer check** should be done by individual review consumers, meaning Veriview does not accredit or endorse any issuers to be valid journals. Veriview serves as a neutral platform for showcasing any peer review credentials. Checks on whether the given journal is a credible one is left to review consumers, where `did:web` was used to make this process easier (RQ5).

The above steps are based on a typical Verifiable Credentials credential exchange where the identities can remain pseudonymous. In our setting, the identities are open (reviewers associate reviews with their profiles publicly). Therefore, by requiring the holder information (`author` of the review) to be included in the credential when exchanging credentials, it is possible to skip the **presenter authentication**, **holder check**, and **presentation verification**. In other words there is no need to wrap the credentials in a presentation. By checking the `author` information such as the `id` and `email` it is possible to make sure that the credential holder and the researcher that is adding the review to his profile are the same person.

In this case, a DID is not required as credentials don't need to be wrapped in a presentation and signed with a key that is associated with a DID. A simple check between the identifier/e-mail in the credential and the user identifier/email will be sufficient to authenticate the holder. A researcher can still associate a DID with their Veriview account by signing a challenge, and add the reviews with the DID as the `author` identifier to their profile. An alternative is to use a centralized identifier such as ORCID or an email for presenter authentication. This, however, requires a degree of trust in Veriview as the platform needs to associate a researcher account with an ORCID account with a single sign-on, or with an email by sending a verification email. Nevertheless, this is a reasonable level of trust as ORCID profiles are open and emails of researchers are also usually publicly available.

Peer Review Credential Derivation

Credential derivation is the key functionality of the system. It allows the selective disclosure of the attributes (RQ6), and hence lets sharing closed reviews publicly without losing the verifiability of the documents. Ideally, this step is executed by the holder's wallet and the original credential does not leave the wallet. If the wallet supports the signature scheme the credential is issued in, the user would select the attributes of the peer review they would like to disclose and the wallet will generate the derived credential with a zero-knowledge proof.

For instance, a review author may have the review credential in Listing 3.1 issued and would like to share their review publicly. If the review was a blinded review, the information shared must not identify the researcher as the reviewer of the manuscript they reviewed. With a review credential signed with `BbsBlsSignature2020` they can decide to only include the `author`, `journal`, `id`, and `type` fields of the `credentialSubject` and exclude `manuscript`, `content` etc. They can generate the derived credential in Listing 3.4. This document contains the selected attributes of the original credential, but different than the original credential, its `proof` does not contain a signature signed by the issuer in its `proofValue`. Instead, the value is a zero-knowledge proof that the holder of this derived document has the knowledge of a valid signature of the original document.

Listing 3.4: Selectively Disclosed Peer Review Credential

```
{
  "@context": [
    "https://www.w3.org/2018/credentials/v1",
    "https://raw.githubusercontent.com/kuzdogan/peer-review-verifiable-
        ↪ credentials-thesis/main/code/PeerReview.json",
    "https://w3id.org/security/bbs/v1"
  ],
  "id": "https://journalx.com/reviews/60afb3a10c601a002c8a43fe/credential",
  "type": [
    "PeerReviewCredential",
    "VerifiableCredential"
  ],
  "description": "A Verifiable Credential representing a peer review that is
      ↪ done for a scholarly article.",
  "name": "Peer Review Credential version 0.1",
  "issuanceDate": "2021-05-27T15:33:28.743Z",
  "issuer": "did:web:journalx.com",
  "credentialSubject": {
    "id": "https://journalx.com/reviews/60afb3a10c601a002c8a43fe",
    "type": "PeerReview",
    "author": {
      "id": "did:key:z6MkpTHR8VNsBxYAAWHut2Geadd9jSwuBV8xRoAnwWsdvktH",
      "type": "PeerReviewAuthor",
      "email": "john@uni-example.edu",
      "familyName": "Doe",
      "givenName": "John"
    },
    "journal": {
      "id": "https://journalx.com/",
      "issn": "2046-1402",
      "name": "International Journal of X"
    }
  },
  "proof": {
    "type": "BbsBlsSignatureProof2020",
    "created": "2021-07-05T12:55:25Z",
    "nonce": "1kQgiDOXEyLc9qr3UX83C1mFip6jIQzCch0+
        ↪ j0iSUsKs32N8Ewokaxgtggd7zMWiDks=",
    "proofPurpose": "assertionMethod",
    "proofValue": "ABwHD/4/h4RPDqsdnm7LiAxQ7joN8tYJJP+pUWiFRjSUwuDwLNH3f53ZC+
        ↪ yD7V62KAlvxskPhmSLIGB42pEnNwWUULlrTFxC...37t6cRsCjePM39bj+ddfkELtV+
        ↪ s04uvVTV/aHbWIuTssPeHzC43U+ho5won/K0kmG/4
        ↪ Xx2g0ZgdZtk7tq4Ux4P49eUZSAtw93CHY6/
        ↪ IgjnCIg3aLV5j8rxKxDp1782dHCUaFPt2anY3YVodjKQez6rdu9phbSdxebqFq9",
    "verificationMethod": "did:web:journalx.com#credentialsKey"
  }
}
```

Adding Reviews to Veriview

To add a review to their profile, a logged-in user would request a credential exchange in their Veriview profile. Next, they will receive instructions to how to do a credential exchange with the Veriview platform. This usually comes in form of a QR code that can be scanned by the user's wallet. The reviewer then chooses which review to share in their wallet, and create a selectively disclosed credential if the review is a blinded review. The wallet will securely transfer the credentials to Veriview, which performs several checks on the review credential before adding it to the user's profile.

First the platform needs to check if the review has been already added to the user's profile. This can be done with the review identifier which is the `id` field in the `credentialSubject`. This identifier can be an internal identifier set by the journal, or a DOI. It is important that the value of this field is consistent across multiple review credentials issued by the journal to avoid a review being added more than once. Additionally, this identifier should not be visible to the manuscript author during the review process to avoid possible identification of the reviewer by the manuscript author.

Next, Veriview will perform a verification on the credential. It will retrieve the contexts and will check if the platform supports all contexts found in the credential. This includes the VC context, any security context used by the signature algorithms (in our case the BBS+

signature vocabulary), and the peer review vocabulary used. A peer review vocabulary is also provided in the design, but as stated the design supports extensions or the usage of different peer review vocabularies. If that is the case, these contexts need to be whitelisted by Veriview. Following the retrieval and check of the contexts, the syntax of the document will be checked according to the JSON-LD grammar (Sporny, Longley, Kellogg, et al., 2020). Next, the **credential verification** will be performed. The identifier of the issuer will be resolved and the associated public keys will be retrieved. Using the key stated in the field `verificationMethod`, the signature of the document in `proofValue` will be validated with the signature suite stated in the credential.

If the credential is verified with the issuer key, Veriview will check if the intended holder of the credential is the current Veriview user. As stated, instead of creating a verifiable presentation, this can be done by checking the user identifier or email on Veriview against the user identifier or email in the uploaded credential. If there is a match, this means the holder of the credential and the user are the same persons. Finally, the review and the credential gets added to the user profile and becomes available for the review consumers' use.

3.2.3 The Role of Distributed Ledgers

Distributed ledgers are widely used in the SSI implementations (van Bokkem, Hageman, Koning, et al., n.d.). The properties of blockchains such as trustlessness, and censorship resistance (Di Francesco Maesa & Mori, 2020) makes them a good candidate as a base for a user-centric identity system (Cameron, Posch, & Rannenberg, 2009). However, due to their publicity and immutability, no personal data should reside on public blockchains (Kondova & Erbguth, 2020).

As of what goes onto a blockchain in such a credentials system, there are two things. First, the contexts and schemas would benefit from high availability and the immutability of blockchains. These documents should not be changed (without versioning) and therefore the immutable distributed ledgers are a natural choice. Alternatively, content addressed storages such as IPFS can be used to ensure the immutability of files. Also, since these documents are widely and commonly used by stakeholders of a VC system, they will benefit from the high availability of distributed ledgers. For instance, if the W3C server, which currently serves the VC base context goes offline, it won't be possible to fetch the context and therefore to verify credentials, unless the context is cached. Additionally, hosting contexts and schemas on a public ledger enhances the privacy as the verifier would not contact the issuer when verifying, and the issuer will not be able to correlate different requests. For the current use case, however, this is not a major concern.

Second, the identities and their associated keys can be stored on blockchains. There exists many DID methods based on distributed ledgers (Steele & Sporny, 2021). However, as stated, identities on blockchains are isolated and need to be connected with the real world identities. This requires an additional step and therefore is not the preferred DID method in this work.

3.3 Prototype

A working proof of concept application is developed to demonstrate the technical feasibility of the proposed solution. The source code is open and available at GitHub[4]. Thanks to the vibrant community around VCs and SSI, and existing open source libraries it was possible to create a working prototype. The implementation mainly relies on the jsonld-signatures-bbs library[5] by MATTR global[6] which is a cryptographic suite of BBS+ signatures to sign, verify, and selectively disclose JSON-LD documents. Since VCs adopts JSON-LD as one of its representation formats, the library can be used for VC implementations as well.

To simulate a typical peer review workflow two different applications were developed: a simple journal management system for submitting and reviewing manuscripts, and a peer review showcasing platform that accepts BBS+ signature peer review verifiable credentials. An overview of the prototype is given in Figure 3.3

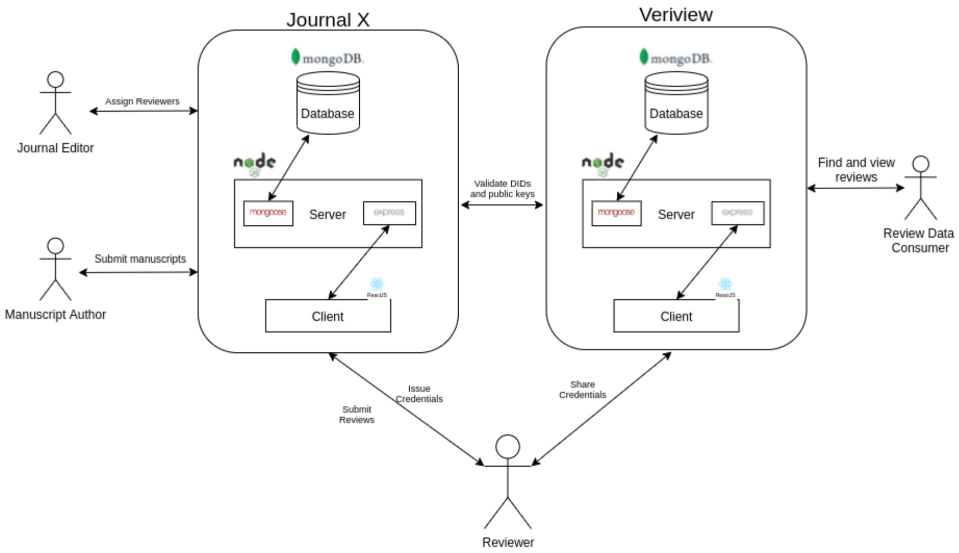


Figure 3.3: Overview of the architecture of the prototype

[4] https://github.com/kuzdogan/peer-review-verifiable-credentials-thesis
[5] https://github.com/mattrglobal/jsonld-signatures-bbs
[6] https://mattr.global/

3.3.1 Journal X

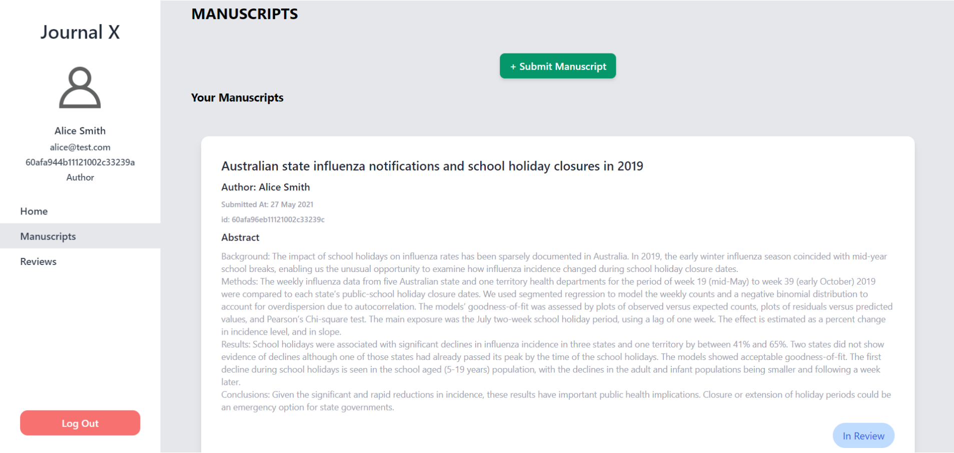
Journal X is the simulated journal management system. Researchers can create an account and submit a manuscript to the journal. The prototype is deployed at https://journalx.herokuapp.com. The application is built on a MERN stack. The MongoDB database stores the `User` and login `Token` data, in addition to the `Manuscript`, `Review`, and the `ReviewTask` data. The CRUD operations are done through the Mongoose driver that runs on the NodeJs Express server.

As the issuer identifier in the credentials DIDs are used. The preferred DID method is `did:web` and the DID of the implemented journal is `did:web:journalx.herokuapp.com`. The document contains the public keys belonging to the journal that are used in credential verification. The DID document is given in Listing 3.5.

Listing 3.5: Journal X DID document

```
{
  "@context": ["https://www.w3.org/ns/did/v1", "https://w3id.org/security/bbs/
      ↪ v1"],
  "id": "did:web:journalx.herokuapp.com",
  "assertionMethod": [
    {
      "id": "did:web:journalx.herokuapp.com#credentialsKey",
      "type": "BbsBlsSignature2020",
      "controller": "did:web:journalx.herokuapp.com",
      "publicKeyBase58": "23
          ↪ V58StUorHjCjukwEfuyvSMDAisf5sgxKvBCAyt3jQTD5zVCw57hao
          ↪ qotHxbqQQZ5WmruofpXUfSNDEVv9gfHE7sFD4fULfhESpJC2FyH2
          ↪ CNaga1Tuzr6VpMcAfUvo3BYGA"
    }
  ],
  "verificationMethod": [
    {
      "id": "did:web:journalx.herokuapp.com#credentialsKey",
      "type": "BbsBlsSignature2020",
      "controller": "did:web:journalx.herokuapp.com",
      "publicKeyBase58": "23V58StUorHjCjukwEfuyvSMDAisf5sgxKvBCAyt3jQ
          ↪ TD5zVCw57haoqotHxbqQQZ5WmruofpXUfSNDEVv9gfHE7sFD 4
          ↪ fULfhESpJC2FyH2CNaga1Tuzr6VpMcAfUvo3BYGA"
    }
  ]
}
```

In Journal X, a researcher can view their manuscripts' statuses as in Figure 3.4 and submit a manuscript that they want to be published in the form page upon clicking "Submit Manuscript".



Australian state influenza notifications and school holiday closures in 2019

Author: Alice Smith

Submitted At: 27 May 2021

id: 60afa96eb11121002c33239c

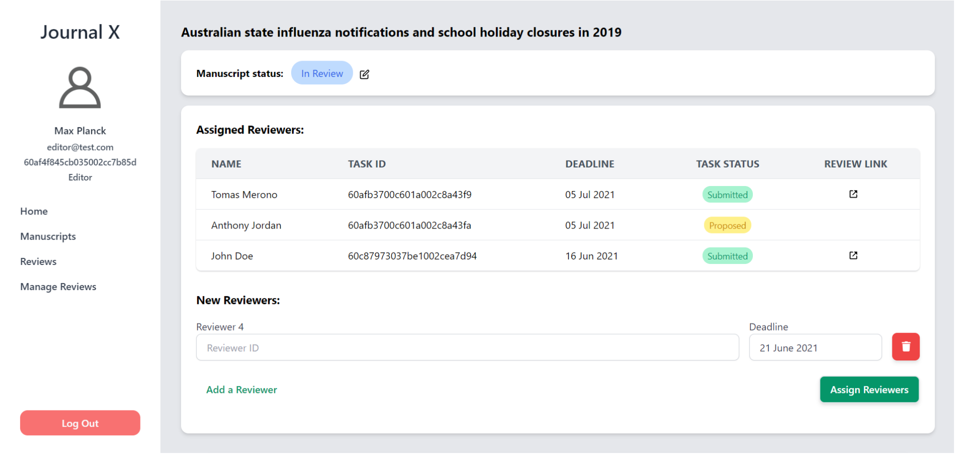
Abstract

Background: The impact of school holidays on influenza rates has been sparsely documented in Australia. In 2019, the early winter influenza season coincided with mid-year school breaks, enabling us the unusual opportunity to examine how influenza incidence changed during school holiday closure dates.
Methods: The weekly influenza data from five Australian state and one territory health departments for the period of week 19 (mid-May) to week 39 (early October) 2019 were compared to each state's public-school holiday closure dates. We used segmented regression to model the weekly counts and a negative binomial distribution to account for overdispersion due to autocorrelation. The models' goodness-of-fit was assessed by plots of observed versus expected counts, plots of residuals versus predicted values, and Pearson's Chi-square test. The main exposure was the July two-week school holiday period, using a lag of one week. The effect is estimated as a percent change in incidence level, and in slope.
Results: School holidays were associated with significant declines in influenza incidence in three states and one territory by between 41% and 65%. Two states did not show evidence of declines although one of those states had already passed its peak by the time of the school holidays. The models showed acceptable goodness-of-fit. The first decline during school holidays is seen in the school aged (5-19 years) population, with the declines in the adult and infant populations being smaller and following a week later.
Conclusions: Given the significant and rapid reductions in incidence, these results have important public health implications. Closure or extension of holiday periods could be an emergency option for state governments.

Figure 3.4: View and submit manuscripts

Upon submission, a review process has been initiated for the manuscript. The editor can assign reviewers for the manuscript and change the publication status of the manuscript according to the reviews as in Figure 3.5. Users can see their assigned reviews (Figure 3.6) and submit the review through the form page. The review includes an optional title, the content, an optional competing interest statement and a recommendation such as "Accept", "Minor Revision", "Major Revision" or "Reject". Finally they can see their submitted reviews as in Figure 3.7 and download the verifiable credential by clicking "Issue Credential".

When the credential is issued, it is downloaded to the reviewer's device as a file in `.jsonld` format. Ideally these credentials are stored encrypted in a credential wallet or another dedicated application and only leave the application after deriving the credential. However, the prototype does not include a wallet since there are no existing ready to use wallet applications that support BBS+ signatures and credential derivation. Also, the credential exchange should be mediated by a secure protocol. Instead, the users download their credentials plain text and use this file in the platforms. The secure connection is also out of scope of this work and only a HTTPS connection is established between the user and the platforms.



Australian state influenza notifications and school holiday closures in 2019

Manuscript status: In Review

Assigned Reviewers:

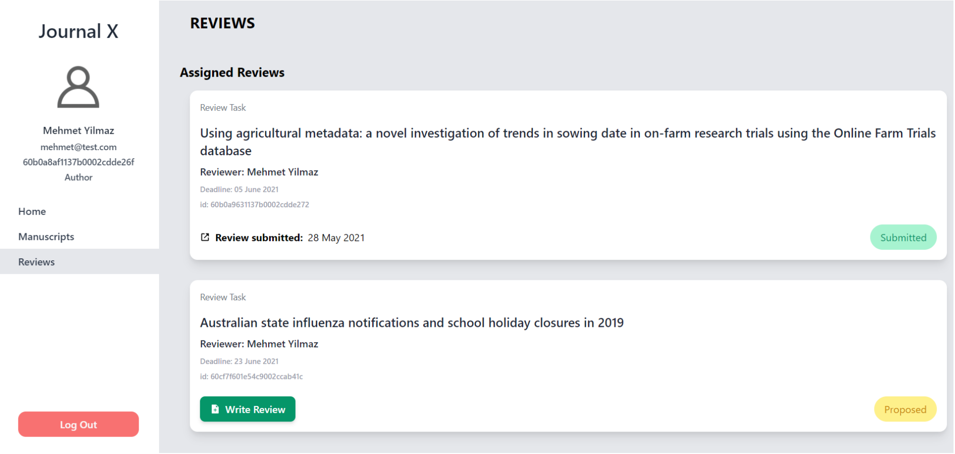
NAME	TASK ID	DEADLINE	TASK STATUS	REVIEW LINK
Tomas Merono	60afb3700c601a002c8a43f9	05 Jul 2021	Submitted	↗
Anthony Jordan	60afb3700c601a002c8a43fa	05 Jul 2021	Proposed	
John Doe	60c87973037be1002cea7d94	16 Jun 2021	Submitted	↗

New Reviewers:

Reviewer 4: Reviewer ID

Deadline: 21 June 2021

Figure 3.5: Editor manage review process screen



REVIEWS

Assigned Reviews

Review Task

Using agricultural metadata: a novel investigation of trends in sowing date in on-farm research trials using the Online Farm Trials database

Reviewer: Mehmet Yilmaz

Deadline: 05 June 2021

id: 60b0a9631137b0002cdde272

Review submitted: 28 May 2021

Submitted

Review Task

Australian state influenza notifications and school holiday closures in 2019

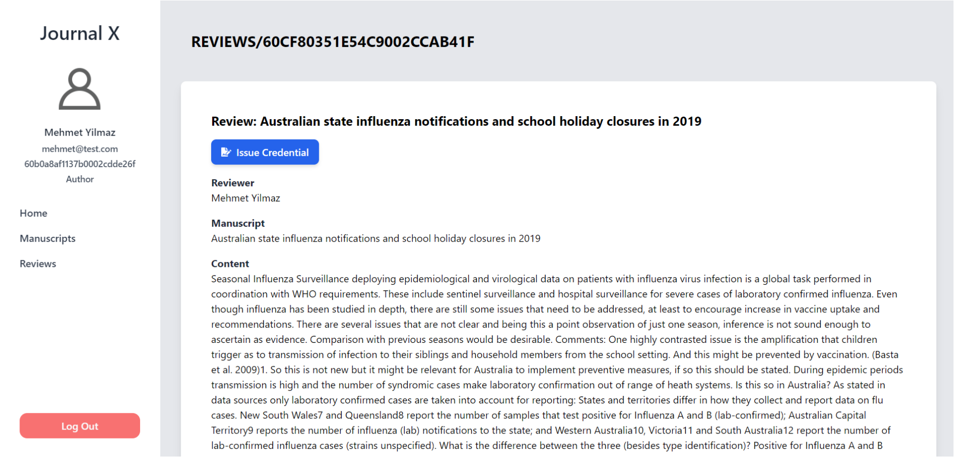
Reviewer: Mehmet Yilmaz

Deadline: 23 June 2021

id: 60cf7f601e54c9002ccab41c

Proposed

Figure 3.6: Reviewer dashboard



REVIEWS/60CF80351E54C9002CCAB41F

Review: Australian state influenza notifications and school holiday closures in 2019

Reviewer
Mehmet Yilmaz

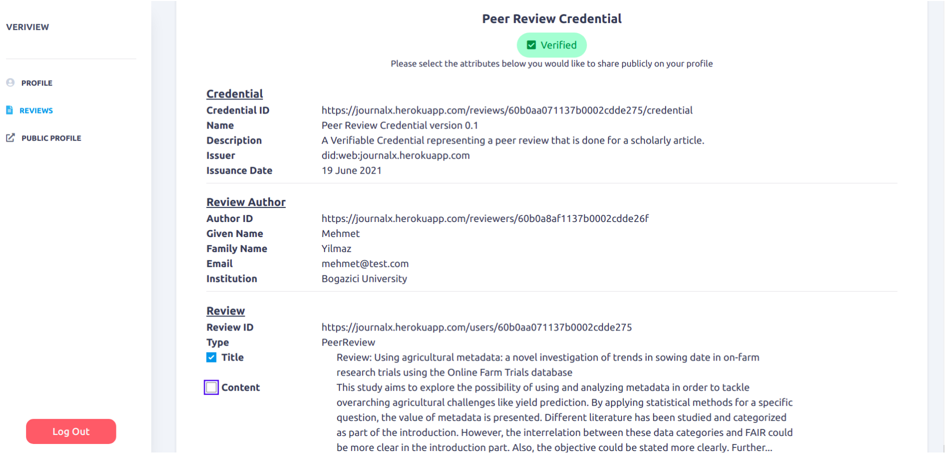
Manuscript
Australian state influenza notifications and school holiday closures in 2019

Content
Seasonal Influenza Surveillance deploying epidemiological and virological data on patients with influenza virus infection is a global task performed in coordination with WHO requirements. These include sentinel surveillance and hospital surveillance for severe cases of laboratory confirmed influenza. Even though influenza has been studied in depth, there are still some issues that need to be addressed, at least to encourage increase in vaccine uptake and recommendations. There are several issues that are not clear and being this a point observation of just one season, inference is not sound enough to ascertain as evidence. Comparison with previous seasons would be desirable. Comments: One highly contrasted issue is the amplification that children trigger as to transmission of infection to their siblings and household members from the school setting. And this might be prevented by vaccination. (Basta et al. 2009)1. So this is not new but it might be relevant for Australia to implement preventive measures, if so this should be stated. During epidemic periods transmission is high and the number of syndromic cases make laboratory confirmation out of range of heath systems. Is this so in Australia? As stated in data sources only laboratory confirmed cases are taken into account for reporting: States and territories differ in how they collect and report data on flu cases. New South Wales7 and Queensland8 report the number of samples that test positive for Influenza A and B (lab-confirmed); Australian Capital Territory9 reports the number of influenza (lab) notifications to the state; and Western Australia10, Victoria11 and South Australia12 report the number of lab-confirmed influenza cases (strains unspecified). What is the difference between the three (besides type identification)? Positive for Influenza A and B

Figure 3.7: View review and issue verifiable credential

3.3.2 Veriview

Veriview is the conceived peer review showcasing platform of the prototype. Similar to Journal X, it is built on the MERN stack. The working application is deployed at https://veriview.herokuapp.com. In addition to a journal account, the users need to create a Veriview account. Once they have an account, they can add the review credentials they obtained from journals to their Veriview profile. To add a peer review, the users are prompted to select the local credential file on their device. The input credential will be parsed and verified on the application. The verification at this stage is on the original credential, and the user will be able to derive a credential in the next steps. The application will first fetch the contexts (unless they are cached), and check the syntax of the document. Following, it will fetch the issuer document, which in our case is the Journal X's DID document. Since it is a `did:web` identifier, it will fetch the DID document at https://journalx.veriview.com/.well-known/did.json. Next, the signature on the credential, which is under the attribute `proof` will be validated against the public verification key of the DID document. If all steps succeed, the document will be marked verified with a green check on top as in Figure 3.8



Peer Review Credential

☑ Verified

Please select the attributes below you would like to share publicly on your profile

Credential

Credential ID	https://journalx.herokuapp.com/reviews/60b0aa071137b0002cdde275/credential
Name	Peer Review Credential version 0.1
Description	A Verifiable Credential representing a peer review that is done for a scholarly article.
Issuer	did:web:journalx.herokuapp.com
Issuance Date	19 June 2021

Review Author

Author ID	https://journalx.herokuapp.com/reviewers/60b0a8af1137b0002cdde26f
Given Name	Mehmet
Family Name	Yilmaz
Email	mehmet@test.com
Institution	Bogazici University

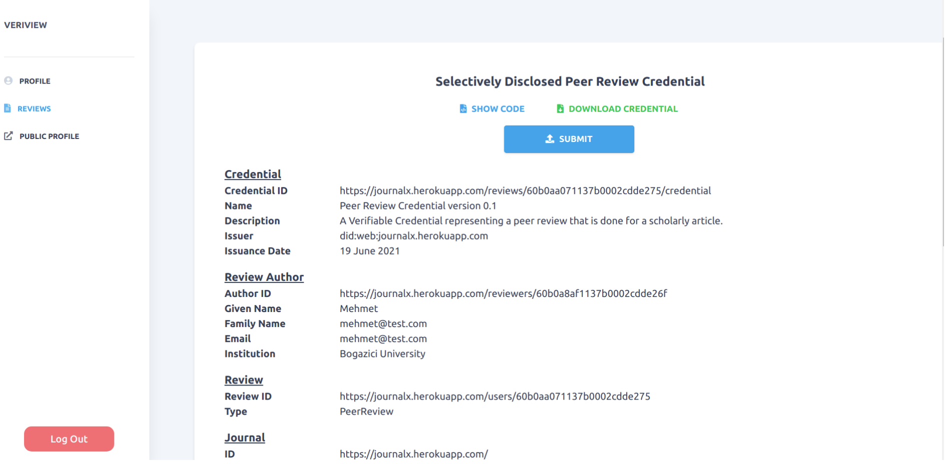
Review

Review ID	https://journalx.herokuapp.com/users/60b0aa071137b0002cdde275
Type	PeerReview
☑ **Title**	Review: Using agricultural metadata: a novel investigation of trends in sowing date in on-farm research trials using the Online Farm Trials database
☐ **Content**	This study aims to explore the possibility of using and analyzing metadata in order to tackle overarching agricultural challenges like yield prediction. By applying statistical methods for a specific question, the value of metadata is presented. Different literature has been studied and categorized as part of the introduction. However, the interrelation between these data categories and FAIR could be more clear in the introduction part. Also, the objective could be stated more clearly. Further...

Figure 3.8: Adding the review credential to Veriview and selecting attributes

Here, the users can choose which attributes of a review they want to share publicly on their profile. For instance, typically a blinded review should not contain any information that would identify the review, meaning the review date, title, content, the manuscript title, and the manuscript abstract should be excluded. The interface does not allow users to exclude some fields such as the credential issuer, issuance date, review id, and review author information.

After selecting the attributes to be shared, a new credential will be derived from the original credential, which only contains the chosen attributes and a `proof` attribute of type `BbsBlsSignatureProof2020`. This proof is different than the signature of the original document, and is a zero-knowledge proof that the holder of this document knows a valid signature over the complete credential that is issued by the same issuer. The users can review the derived credential and add it to their profile by clicking "Submit". It is also possible to view the raw document in JSON-LD format by clicking "Show Code", and download the derived credential (Figure 3.9).



Selectively Disclosed Peer Review Credential

Credential	
Credential ID	https://journalx.herokuapp.com/reviews/60b0aa071137b0002cdde275/credential
Name	Peer Review Credential version 0.1
Description	A Verifiable Credential representing a peer review that is done for a scholarly article.
Issuer	did:web:journalx.herokuapp.com
Issuance Date	19 June 2021
Review Author	
Author ID	https://journalx.herokuapp.com/reviewers/60b0a8af1137b0002cdde26f
Given Name	Mehmet
Family Name	mehmet@test.com
Email	mehmet@test.com
Institution	Bogazici University
Review	
Review ID	https://journalx.herokuapp.com/users/60b0aa071137b0002cdde275
Type	PeerReview
Journal	
ID	https://journalx.herokuapp.com/

Figure 3.9: The selectively disclosed peer review credential

Finally users can view their profiles, and their profiles are publicly available at their unique URLs. On this page the review consumers can view the review contributions of a researcher.

Comparison to the conceptual design

The prototype is not a complete implementation of the conceptual design and only serves the purpose of demonstrating the technical feasibility of the conceived system, in particular the VC implementation of peer reviews including the issuance, verification of the credentials, and the selective disclosure with the zero-knowledge proofs. Below are the main differences between the original design and the implemented prototype.

- **Wallet:** Verifiable credentials normally should be stored and managed in wallet applications as they contain personal information. Another reason is to be able to complete other actions in VC exchanges such as establishing a secure channel, selective disclosure, verification of credentials or wrapping credentials into verifiable presentations. The implementation does not include a wallet application and the mentioned steps are either omitted or done by different parts of the application. As a secure channel only HTTPS connection is available and users directly download the credentials issued by the journal. As discussed, usage of verifiable presentations in credential exchange can be skipped by checking the identifier/email information of the review author. Additionally the Veriview application is used for credential verification, and selective disclosure. When a user adds a credential, the client side application fetches the `issuer` DID and verifies the credential. Users can also derive selectively disclosed credentials on the client side without the credentials being sent to the server.

- **Review Invitation:** In a typical review process, journal editors invite researchers to review manuscripts. Researchers can accept or reject this invitation. However, in the prototype the editor can directly assign researchers as reviewers.
- **Credential Issuance:** Upon receiving the peer review journals may decide not to immediately issue peer review credentials to review authors. Journals may wait until the decision to publish the manuscript has been made or until the manuscript is published. In the prototype review authors can immediately download their review credentials.
- **Duplicate Reviews:** When users are adding a review credential to their profile, it should be checked if the review has already been added to avoid showing a review contribution multiple times as if they are different reviews. This can be simply done by requiring the identifier of the review in the credential, which is unique and consistently assigned by the issuing journal. The prototype does not complete this check to allow first time users test out selective disclosure without needing to write a new review, but it is a fairly simple change.
- **Reviewer Identifier/Email Check:** As discussed in the design section, it is possible to skip some extra steps in the VC verification by checking the review author identifier/email when adding a review to the Veriview. Even though users provide an email when signing in to the Veriview prototype, this check is not made as it requires an implementation of email and DID verification, and it is out of the scope of the prototype.

4 Evaluation

This section provides an evaluation of the designed artifact in two ways. In the previous section, seven requirements have been defined for the designed system. First, it will be discussed how the designed system fits in these requirements. Second, a qualitative evaluation of the system will be presented. For this part of the evaluation, one hour interviews with five different researchers with peer review experience were conducted. The Technology Acceptance Model (TAM) is used as a framework to assess the system usage qualitatively. The responses by the interviewees are categorized under TAM variables and interpreted to determine their intention to use of the system. According to the responses, a basic acceptance model is proposed. Various insights gained during the interviews about the system and peer reviewing in general are also shared.

4.1 Evaluation of Design Requirements

Based on open science principles and the problems discussed, seven requirements were defined for the system:

- RQ1: Verifiability
- RQ2: Transparency
- RQ3: Open Data
- RQ4: Open Standards
- RQ5: Direct Trust
- RQ6: Selective Disclosure
- RQ7: Compatibility

1. Verifiability

Verifiability, in short, encompasses the ability to check if a peer review has really taken place and the presented information about the peer review is correct. The designed system is based on Verifiable Credentials, which makes use of the Linked-Data Proofs or JSON Web Tokens that allows the verification of credentials using digital signatures. By resolving the `issuer` (journal) identifier, their public keys can be retrieved and the credential can be verified.

2. Transparency

The designed system improves upon the existing ones in numerous ways in terms of transparency. First of all, the verification of the peer reviews is transparent, that is anyone can take the existing data and verify that the peer review credential is actually issued by the given journal, and that it is authentic. Current showcasing platforms verify the reviews themselves and mark the reviews as verified without information on how this verification is done. Also, the Veriview platform can complete the verification steps and inform the users on its user interface that the review is verified. By open sourcing the code this process is also kept transparent.

3. Open Data

Even though the nature of blinded peer reviews prevents complete openness of the data, the system makes it possible to keep as much data of peer reviews as possible open without losing verifiability. Additionally, the data stored in Veriview is identical to what is publicly available.

4. Open Standards

The system is based on open standards under development such as Verifiable Credentials, Decentralized Identifier, JSON-LD. The platforms are open sourced and anyone can easily create a similar platform. This would avoid future vendor lock-in and further contributes the openness of the system.

5. Direct Trust

The peer review credentials are issued directly by journals and the verification is also done through journal keys. The showcasing system only serves as a platform to share and host the credentials, and requires minimal trust.

6. Selective Disclosure

By using Linked-Data Proofs with BBS+ Signatures, it is possible to derive credentials with a subset of the attributes, and with a zero-knowledge proof that ensures the knowledge of the original credential and a valid signature. This enables review authors to only share the non-identifiable information of a review without losing verifiability.

7. Compatibility

The proposed system allows the extension of the proposed peer review vocabulary or the use of different vocabularies instead. This enables to accommodate the data model of the credentials to different peer review processes but also keeps the interoperability by having the vocabularies published.

4.2 Interviews

4.2.1 Method

For the qualitative evaluation of the work, five different researchers with peer review experience were interviewed. All participants were male. Four participants were invited for interviews through existing connections. Additionally, to at least interview one frequent Publons user, the researchers with most reviews under the "Researchers" tab on Publons were browsed. Among them 20 researchers were contacted who have at least one publication with an arbitrary order. In the end Interviewee 5 accepted the request to interview. Additional details on interviewee profiles are given in Table 4.1. Here the number of publications are taken from their Google Scholar profiles, and their peer review numbers from their statements if a Publons profile is not available. The interviews took around one hour, were recorded and transcribed with the interviewees' consents. The interviews encompassed first a general discussion around the interviewee's peer review experience and their perspectives, followed by an introduction to existing review showcasing platforms, in particular Publons, and their experience if they had any. Next, the conceptual design of the system is presented. The interviewees were then given a hands-on experience of the prototype and they were asked to complete the basic user flow of the application. Finally, their review of the system is solicited.

The interviews were run as free dialogues and did not follow a strict structure besides the flow described above. However, the following or similar questions were asked to interviewees over the course of the interviews:

- Could you please introduce yourself and detail your peer review experience?

	Field	Gender	Publications	Peer Reviews	Publons user?
Interviewee 1	Computer Science	Male	9	5-10	No
Interviewee 2	Political Science	Male	12	19	Yes
Interviewee 3	Computer Science	Male	13	not stated	No
Interviewee 4	Theoretical Biology	Male	52	40+	No
Interviewee 5	Additive Manufacturing	Male	97	816	Yes

Table 4.1: Interviewee details

- How would you describe the peer review culture in your field?
- What motivates you to do the peer review for a manuscript?
- Has there been a case where you presented your reviews in an academic resume, or that it would be beneficial if you could present it?
- Are you using review showcasing platforms? If yes, could you describe your experiences?
- What consequences may arise in the future that Publons is the only owner of the peer review data?
- Do you think the value added by Veriview exceeds the complexity it creates?
- What might be a reason to share or not to share your peer reviews on such a platform?
- Who might be interested in consuming the peer review data on Veriview?

4.2.2 Summary

A recurring theme across all interviews was the lacking constructiveness and quality in some reviews and that some review authors don't seem to invest sufficient time to write reviews that will improve the manuscript. This seems to dishearten the researchers who try to write good reviews. Another discouraging experience mentioned by interviewees were the cases where the interviewees see a paper they carefully reviewed with constructive feedback being published elsewhere without any of their input being taken into account. Nevertheless, all but one interviewees state reciprocity and a sense of duty as the main motivations to do peer reviews. The second common motivation stated has been the early access to research in their fields and having an idea what other researchers are working on. These are in line with the existing research and surveys (Publons, 2018; Squazzoni, Bravo, & Takács, 2013; Taylor & Francis, 2015; Ware, 2008).

The interviewees all include their review or editorial work in their academic resumes, but usually this information is given a low priority without much detail and placed at the bottom of the resume. Because as Interviewee 1 stated: "there is not really a culture that the reviews become part of your CV or of your reputation". If this was the case, for instance reviewing in a high ranking journal would increase the reputation of scientists, then the reviewers would invest more resources to reviewing, he also explains. Interviewee 4 also affirms that these contributions are not deemed important. Interviewer 3 pointed out having this information on the resume demonstrates that you are connected with certain communities and having recently a best peer reviewer prize awarded, he became aware that it is nice to have this type of work published. Interviewee 5 brought the value of these records into question as it does not convey any information on the quality of the review and reminded that many reviewers don't really put much effort. Interviewee 1 mentioned that including this field shows that one engaged with the broader science, and it contributes to their periodical evaluations. But at the same time, institutions don't want researchers to spend much time doing peer review and their main focus is publications and grants a researcher has, and researchers' incentives are not aligned to do reviews but to publish papers and get grants, as Interviewee 4 mentioned. "The peer review is really, in objective terms, a waste of time. It is really an altruistic thing you do, I think", he said.

Even though most interviewees include peer reviews in their resume, some of them didn't think verification would be a necessity. "I'm sure people inflate their CV's" said Interviewee 2, "...but I don't think there's much incentive to lie with your peer reviews.". Interviewee 3 said he is not aware of anyone falsely claiming he/she reviewed for a journal, or if there is a motivation to do that. He also thinks Publons, despite being a trusted third-party, is not incentivized to publish inaccurate data as this is their core business and such an action would impair their reputation heavily.

On the one hand, these statements show that researchers care for their peer review work and want to demonstrate their efforts but the larger scientific community doesn't seem to regard review service as a measure in practice. More visibility and availability of reviews would be a positive change for researchers in this sense. However, the perspectives on the unnecessariness of proofs, unimportance of reviews, and that no one would lie with their review work demonstrates the need for further validation of the significance of the problem.

When asked about Publons, the interviewees said they heard other people using it. The active users started using it after receiving an automatic invitation following a review they submitted, and they denote that they don't put much effort on their profiles, and don't actively add reviews.

When questioning about the consequences of Publons being the only owner of the peer review data, contrasting answers were received. The interviewees mostly expressed they didn't consider this before. Two of the reviewers didn't see this as a problem, one even favored centralization that it brings more accountability and makes it easier to manage the data. Also, some interviewees don't consider that Publons has all the data but only the ones shared by the users, therefore that it does not strictly control the data and only collects a portion of it. However, concerns have been raised that if the platform becomes a de facto standard for review recognition, it could create a harder vendor lock-in, similar to what the scientific community experienced in the acquisition of Mendeley by Elsevier[1]. The fact that this data is controlled by a commercial entity is not necessarily bad, but something to be cautious of, especially that in the future this data can be monetized in various ways that won't be favored from an open science standpoint. Observably for the interviewees with interest in open science practices and decentralization, this concern was higher. Another decentralization aspect was brought up by Interviewee 3 that this may cause established reviewers to get more invitations and others less, and a more equal distribution of the review work is favored. Such inequalities are already apparent in peer review (Hochberg, Chase, Gotelli, et al., 2009; Publons, 2018; Ware, 2008; Warne, 2016) and the use of this data for reviewer matching could exacerbate this. This might be mitigated by including training for fresh reviewers, and utilizing different data for matching such as connections and research field.

Later the conceptual design was introduced to the interviewees and their understanding of the concept was observed. A common confusion was around how the credentials are issued and how the verification works. However, without needing to explain the technical details, they were able to understand that the proof shows the authenticity and the integrity of the review, and that a credential with a subset of the attributes of the original credential can be created. All interviewees agreed that the designed artifact, as it is, is more complex than the existing platforms, but they could easily see that these complexities can be abstracted away from the user by a Researchgate plugin or similar (Interviewee 3) or automating the Veriview-journal interactions (Interviewee 4). The Interviewee 1 and 5, both Publons users, emphasized the need of effortlessness on these steps. Since researchers, currently, don't put too much value on showing their reviews, these steps have to be as easy as possible. Interviewee 1 pointed out the typical learning curve in SSI systems which includes making users aware that the credentials and keys are under their responsibility, and the cases of wallet loss and key management need to be considered. Even though in the system DIDs are

[1] https://www.mysciencework.com/omniscience/elsevier-takes-over-mendeley-and-you-what-do-you-think

not a requirement for authors, credential management can become a usability issue as stated.

When asked who would become a review data consumer, journals and journal editors looking for reviewers were the common answers. Currently manuscript authors are sometimes asked to recommend reviewers and they can also benefit from the availability of this data, Interviewee 2 suggested. He also added researchers that need to regularly report their work can include their review efforts through systems like this. Additionally, Interviewee 3 stated such a platform can benefit researchers that would like to improve their writings and reviewing skills by providing access to good reviews. Institutions can also make use of this data to better asses the researchers and see their contributions to the larger community, Interviewee 4 suggested.

4.2.3 Findings

Based on the reviews of the interviewees, key findings regarding the system design and prototype are listed below:

- **Too much user involvement:** Current prototype requires users to download the credentials and upload to Veriview, as well as the design gives agency to users for managing their credentials. This process should be as automatized as possible.
- **Importance of reviews:** The discussions reveal that researchers don't attribute much importance to their review records. Although surveys indicate a demand for the higher recognition of peer reviews, at the current state it is not considered as a primary output of a researcher by institutions and the community, and hence researchers might not be motivated enough to showcase their reviews.
- **Need for verification:** Commonly the interviewees state they don't think anyone would falsely claim reviews. This implies peer review verification may not be a relevant problem currently.
- **Open science aspect:** The interviewees mostly agreed or were indifferent with the concerns over the existing showcase platforms in terms of open science.

4.3 Acceptance Model

The use of information technologies in workplaces and organizations has been increasing significantly, improving productivity across many aspects. Scientific publishing is no exception (Ware & Mabe, 2015, p. 132). Understanding the adoption of new technologies, therefore, is a major research interest and an established field. The Technology Acceptance Model (Davis, 1989; Davis, Bagozzi, & Warshaw, 1989; Fred D. Davis, 1985) became a widely used framework for explaining the user acceptance and its validity has been tested many times since over a quarter century (Marangunić & Granić, 2015). TAM proposes the perceived usefulness and the perceived ease of use as the main determinants of the attitude toward using the technology which also influences the behavioral intention to use. The model is rather parsimonious in number of variables, and different extensions to the model have been proposed (Marangunić & Granić, 2015).

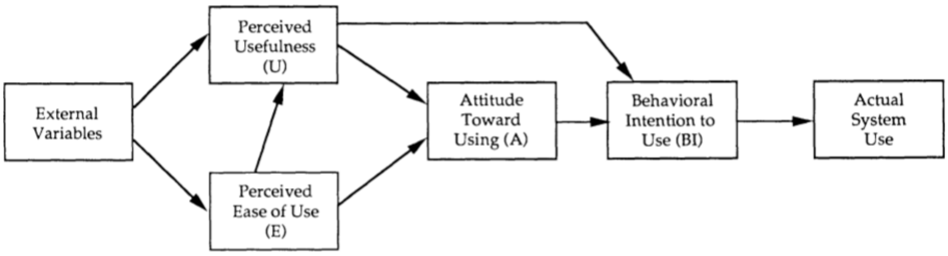

External Variables
Perceived Usefulness (U)
Perceived Ease of Use (E)
Attitude Toward Using (A)
Behavioral Intention to Use (BI)
Actual System Use

Figure 4.1: Technology Acceptance Model (Davis, Bagozzi, & Warshaw, 1989)

Based on the findings from the interviews the variables are discussed that would influence the perceived usefulness and the perceived ease of use of the designed system and an acceptance model is proposed. As users only review authors are considered but there are many potential types users such as journals, universities, research institutes etc.

4.3.1 External Variables

Institutional Demand

The interviews reveal that researchers don’t esteem peer review as part of their resume as they don’t feel this information is considered by institutions. It is proposed that the institutional demand for peer review records of a researcher will have a positive impact on the perceived usefulness of the system. With higher such demand, researchers would be more inclined towards showcasing their peer reviews in a verifiable way.

Significance of Peer Reviews

A common statement during the interviews was the insignificance of peer reviews in assessments, tenure, and overall researcher reputation. This was also apparent in how researchers include their review work in their resumes, by only sparing little space for this information.

The disparity of this perception in the scientific community with the peer review's importance in scientific knowledge generation has been discussed in previous sections. The disparity has caught the attention of the community (J. Tennant, 2020; Veríssimo & Roberts, 2013) and the need for more recognition to peer review is being voiced. Researchers expect their institutions to require and recognize peer review contributions (Publons, 2018) and state they would spend more time on reviews if it was recognized (Warne, 2016).

The variable is defined broadly as significance of reviews, as this includes both the value researchers give to reviews, the degree of recognition from institutions, and the attitude of the scientific community towards review work of a researcher. As institutional demand is part of the significance of reviews, it is proposed in the model that the institutional demand positively affects the significance of reviews. Besides, more significance of peer review works of a researcher would increase the need for such peer review showcasing and verification systems. Therefore, proposed is that the significance of reviews will have a positive effect on the perceived usefulness of the technology. Interestingly, this is a chicken and egg problem, where the under-utilization of review recognition platforms are due to peer review's insignificance, and peer review's under-recognition is a result of unavailability of ways to demonstrate peer review work. Put other way, there exist the potential of a virtuous feedback loop: more visibility to peer review may foster peer review's significance and more significance of the process would create more demand to use showcasing platforms.

Open Science Commitment

Open science commitment can be defined as the degree of adoption of open science in a researcher's practices. The designed artifact aims to remove trusted third parties from the review verification process and promote open data and transparency. This aspect is also the main differentiating property of the designed system from the existing ones. Taking this into account and based on the observations during the interviews, it is proposed that open science commitment of a researcher will have a positive impact on the perceived usefulness of the system. This factor would also influence the preference of a user between existing showcasing systems and the designed system.

Active Use Requirement

The majority of the interviewees expressed the need for automation of the user actions on the platform. Researchers don't spend much time on their peer reviews once they write and submit it. As Interviewee 2 said, reviewers just do the review, send it, then move on to other tasks. They don't think about that review anymore. Interviewee 5 also highlighted the importance of effortless usage of the system, saying he also was invited to try an application similar to Researchgate but did not continue using it as he didn't want to get into the trouble. Either the value added by the platform should be evident to put time on platform's tasks or it should be as effortless as possible. Google Scholar, since it is the primary online profile and shows a scientist's publications and citation metrics, is checked regularly by Interviewee 2 but he almost never spends time on his Publons profile. Based on these observations it is proposed that the active use requirement has a negative effect on the perceived ease of use. The most important component of this would be adding the reviews to the user profile. If this step could be automated, the perceived ease of use would highly increase.

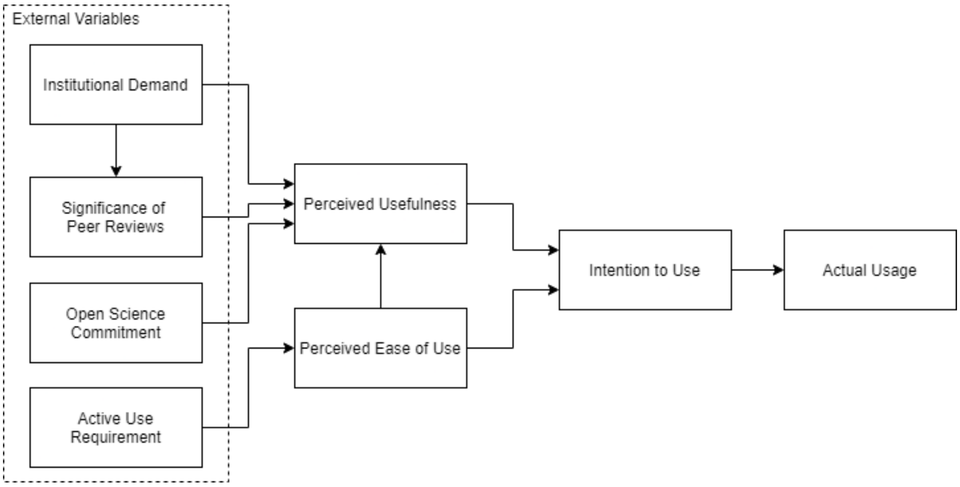


Figure 4.2: Proposed acceptance model for peer review showcasing system

Based on the findings the acceptance model in Figure 4.2 is proposed. The current design requires the reviewer to claim the credentials from their journal and add manually to Veriview. This property falls short in terms of active use requirement and should be improved for a higher perceived ease of use. The rest of the variables are external to the system design and depend on individual users or the wider scientific community.

5 Discussion

Peer review is an essential part of the scientific knowledge creation. At the same time, it is a disputatious topic with different camps on how the process should be done, or what its purpose is. Still, there is consensus on many shortcomings of the process and there is clear room for improvement. An area open for experimentation is the peer review recognition and incentivization. Studies and surveys demonstrate there is a clear expectation from the community to recognize review efforts of researchers and the majority thinks the process will improve with more incentives, but the question remains on how to achieve this and what the unintended consequences will be.

An effort in this direction is the review showcasing platforms, most prominent of them being Publons. As much as they contribute review recognition, here it is argued that such platforms do not align with open science goals and may work against the common benefit of the scientific community. It is also recognized that these problems are rooted in the role these platforms play as trusted third-parties in review verification. To tackle the recognition and incentivization problem, and to avoid the argued problems these platforms may cause, a system was designed that enables verification of peer reviews without a trusted third-party. To best of our knowledge, this work is the first one around this specific problem, and among a few practical works around peer review incentivization.

During the research, the inherent dilemma in the peer review process also became clear. On the one hand, peer review as a scientific process requires transparency and accountability. On the other hand as a scrutinizing process, there is need for anonymity when doing reviews. This dilemma is also at the center of the open vs. blinded reviews debate. Although it does not solve this dilemma, the designed system brings these two ends closer by leveraging emerging standards in the Self-Sovereign Identity space such as Verifiable Credentials and Decentralized Identifiers, and cryptographic protocols of Zero-Knowledge Proofs. A working prototype was also developed that demonstrates the technical feasibility of the solution with existing frameworks and libraries. The design and the prototype of the system also contributes as a reference for future Verifiable Credentials works as there exists few system design and development works in this emerging field.

The interviews reveal several important aspects about the research area and the designed system. First and foremost, with the current degree of recognition and importance given to peer reviews, researchers may not be willing to put much effort on showcasing their peer review records. Therefore, it is crucial to minimize the user input required for such system and automate many processes. Alternatively, the perceived value of showcasing reviews need to be increased. However, this is a much wider problem that requires changing perspectives of institutions, individual researchers, and the scientific community as whole. It was also observed researchers with expressed familiarity with open science practices perceived the system more useful. This feedback was valuable as this is the main value proposition of the system, and that this aspect is the main improvement the designed artifact proposes over the existing systems. Secondly, however, most of the interviewees didn't regard verification of peer reviews as a necessity. This sentiment is connected to the first point above that demonstrating their review records is not worthwhile, and most of the interviewees expressed they don't expect researchers to falsely claim any review experiences. Overall, the depth and the quantity of the interviews were minimal, and these findings suggest further investigation on researchers' attitude towards showcasing reviews would be useful.

Besides, the designed system also has some practical shortcomings. The proposed system require journals to issue peer review credentials. This requirement is a major barrier for adoption as journals must be convinced of the value implementing such a system would bring. Additionally, a very simple peer review process was assumed. As discussed, the process varies a lot among journals. Even though the vocabularies are extensible, there need a degree of agreement to mutual vocabularies. Too much extensibility would break the interoperability in practice. In an ecosystem with many different stakeholders such as peer review, these impose large coordination and governance problems. Stakeholders of peer review are not inclined to change their customs and peer review remains a difficult field to innovate in (J. P. Tennant, 2018, p. 3). The platform also exhibits a cold start problem: the platform is as useful as number of users and the peer review data available on the system. It is quite difficult to attract users to an empty platform. As a workaround, it might be beneficial to bootstrap the platform with existing peer reviews (Interviewee 1) such as open peer reviews or reviews available on Publons. Another open issue is who would be willing to maintain such a showcasing platform. The system is proposed here but running and maintaining the system will have costs associated and it is not considered who would take on those costs. To avoid negative attitudes towards the platform, it would be better if it is run by a non-profit or a joint organization instead of a commercial entity.

The system inherits the advantages of SSI and VC systems such as verifiability, selective disclosure, and open standards. However, the problems of these systems are also inherited. The system as described here gives agency to its users to manage the credentials in a wallet.

If they want to use DIDs, they would also need to manage keys and consider key loss. This is a broader problem in SSI UX and more user friendly solutions are needed for the wider adoption of SSI practices. Nevertheless, the option to avoid user DIDs and the complexities it brings is provided in the system through alternative identifiers such as email or ORCID. Still, the journal identity is based on the journal domain name and does nor provide any information on the legitimacy of the journal. A verifier also needs to verify if they know the journal and its domain name.

The domain based identity provides a degree of affiliation to the real world identity. Using DLTs for identity would require further binding the on-chain identities to real world identities, but would also bring high availability and tamper-proofness to the identities. The decision was made to not use DLTs for identities to be able to use the journal domain names as identifiers. Another possibility of DLT use is the hosting of the contexts and schemas. This implementation is kept out of scope of the prototype but this could be included in future work.

Even if the recognition of peer reviews improves, the fundamental questions remain. What constitutes a good peer review and how can it be measured? As Interviewee 5 suggested, a mere number does not express any information on how much the researcher contributes the science. And as with any metric, this could be easily gamed. How can reviewers be incentivized, or should they be incentivized? Here the need for incentivization was pinpointed based on the findings in the literature but no tangible rewards were suggested in this work. How and if the reviewers should be rewarded is still an open question. As with anything that involves humans, peer review is not perfect either. But it could only improve through further research and experimentation.

6 Conclusion

In this work, a design science research on peer review recognition was presented and a system design was delivered as an artifact. The work initially gave an overview of the peer review. The problems discussed in the literature were introduced, and the currently misaligned incentives were highlighted, that is to publish more and get cited more instead of doing peer reviews. Despite being considered highly important and essential in scientific knowledge generation, scientists are not incentivized to do peer reviews and there are concerns on the implications of this on the quality and the sustainability of the peer review. Further, the problem was investigated and the lack of recognition for the peer review work of the researchers was described. It was argued that this is partly caused by the nature of the practice of blinded reviewing, that requires identities to be hidden and reviews not to be published. The existing platforms were examined that are tackling this problem and current and future problems were identified from an open science perspective. It was observed that these platforms aggregate data by acting as trusted third-party peer review verifiers. From this specific problem the following research question was derived: "How can closed peer reviews be verified without trusted third-parties?"

To answer this question a system using Verifiable Credentials and Zero-Knowledge Proofs was designed and developed. The designed system enables the verification of peer reviews through journals issuing peer review credentials. It also includes an open review showcasing platform where reviewers can add these verifiable credentials without breaking the anonymity of the blinded reviews. A proof of concept prototype was also implemented to show the technical feasibility of the conceptual design.

Overall, this work is a first step in the unexplored space of peer review verification and recognition in the literature. It presents a system that enables the verification of peer reviews without a trusted third-party. It also demonstrates how the state of art standards and zero-knowledge cryptography can be used to benefit peer reviewers. The evaluation suggests further investigation is required in the problem space and the attitudes of researchers towards showcasing reviews. The designed system answers the research question proposed. With the design of the system, several learnings were gained. First, with the current significance of peer review records from researchers' perspective, it is crucial for such a showcasing system to attain minimum user input. Furthermore, there need to be increasing institutional demand for the review records and the system to be perceived useful. Familiarity with open science practices is also found to increase the perceived usefulness of the system. With these variables found, an acceptance model was proposed. It was observed that the designed system also inherits the usability problems currently existing in the SSI applications although some of those could be avoided by using alternative centralized identifiers. This system design with VC and zk-proofs is among few in literature and serves as a reference for future implementations and designs. It also contributes as a system to the larger peer review incentivization problem, and brings light into the potential implications of the current peer review showcasing systems.

Future work can also include the validation of the proposed acceptance model to better understand user behaviour and the potential system usage. Following implementations would benefit from working with real-world publishers and making use of real world data to see how the designed system would adopt, and what problems may arise. It would also uncover how and if the automatization of adding the peer review records can be achieved, which is found to be the main barrier for the user adoption.

List of Figures

List of Tables

Acronyms

API Application Programming Interface. 5, 7, 42

CL Camenisch-Lysyanskaya (signatures). 38

CRUD Create-Read-Update-Delete. 50

DID Decentralized Identifier. 12, 25–27, 39–45, 49, 50, 53, 55, 57, 61, 66, 68

DLT Distributed Ledger Technology. 40, 68

DOI Digital Object Identifier. 47

DSRM Design Science Research Methodology. 10

ECDSA Elliptic Curve Digital Signature Algorithm. 22

EdDSA Edwards-curve Digital Signature Algorithm. 22

GDPR General Data Protection Regulation. 24

HTTP Hypertext Transfer Protocol. 40, 54

IoT Internet of Things. 26

IPFS Interplanetary File System. 9, 48

IRI Internationalized Resource Identifier. 17–19

ISSN International Standard Serial Number. 38

JSON Javascript Object Notation. 16, 17, 35, 57, 73

JSON-LD JSON Linked Data. 12, 16–20, 23, 26, 35, 37, 38, 48, 54, 57

JWT JSON Web Token. 16, 23

MERN MongoDB-Express-ReactJS-Node. 50, 53

ORCID Open Researcher and Contributor ID. 5, 7, 42, 45, 68

PKI Public Key Infrastructure. 40

RDF Rescource Description Framework. 17

RFC Request For Comments. 17

SSI Self-Sovereign Identity. 27, 40, 48, 61, 66–68, 70

TAM Technology Acceptance Model. 56, 63, 71

TLS Transport Layer Security. 22

URI Uniform Resource Identifier. 17, 25, 27, 39

URL Uniform Resource Locator. 17, 35, 38, 40, 42, 54

URN Uniform Resource Name. 17

UX User Experience. 68

VC Verifiable Credentials. iv, 12–17, 20, 23, 27, 30, 35, 39, 40, 42–45, 47, 48, 54, 55, 57, 66, 67, 69–72

W3C The World Wide Web Consortium. iv, 14, 48

YAML YAML Ain't Markup Language. 16

zk-proofs Zero-Knowledge Proofs. 12, 13, 24, 66, 69, 70

Bibliography

Avital, M. (2018). Peer review: Toward a blockchain-enabled market-based ecosystem. *Communications of the Association for Information Systems*, *42*(1), 646–653. https://doi.org/10.17705/1CAIS.04228

Barclay, I., Radha, S., Preece, A., Taylor, I., & Nabrzyski, J. (2020). Certifying provenance of scientific datasets with self-sovereign identity and verifiable credentials. https://arxiv.org/pdf/2004.02796

Baveye, P. C., & Trevors, J. T. (2011). How can we encourage peer-reviewing? *Water, Air, & Soil Pollution*, *214*(1-4), 1–3. https://doi.org/10.1007/s11270-010-0355-7

Benet, J., & Sporny, M. (2021). *The Multibase Data Format* (Internet-Draft draft-multiformats-multibase-03) [Work in Progress]. Internet Engineering Task Force. Internet Engineering Task Force. https://datatracker.ietf.org/doc/html/draft-multiformats-multibase-03

Ben-Kiki, O., Evans, C., & döt Net, I. (2009). Yaml ain't markup language (yamltm) version 1.2. https://yaml.org/spec/1.2/spec.html

Berners-Lee, T., Fielding, R. T., & Masinter, L. M. (2005). Uniform Resource Identifier (URI): Generic Syntax. https://doi.org/10.17487/RFC3986

Bezjak, S., Clyburne-Sherin, A., Conzett, P., Fernandes, P., Görögh, E., Helbig, K., Kramer, B., Labastida, I., Niemeyer, K., Psomopoulos, F., Ross-Hellauer, T., Schneider, R., Tennant, J., Verbakel, E., Brinken, H., & Heller, L. (2018). *Open science training handbook*. Zenodo. https://doi.org/10.5281/zenodo.1212496

Bianchi, F., Grimaldo, F., & Squazzoni, F. (2019). The f3-index. valuing reviewers for scholarly journals. *Journal of Informetrics*, *13*(1), 78–86. https://doi.org/10.1016/j.joi.2018.11.007

Blum, M., Feldman, P., & Micali, S. (1988). Non-interactive zero-knowledge and its applications. In J. Simon (Ed.), *Theory of computing* (pp. 103–112). ACM Press. https://doi.org/10.1145/62212.62222

Boeyen, S., Santesson, S., Polk, T., Housley, R., Farrell, S., & Cooper, D. (2008). Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile. https://doi.org/10.17487/RFC5280

Boneh, D., & Boyen, X. (2004). Short signatures without random oracles. *International conference on the theory and applications of cryptographic techniques*, 56–73.

Bornmann, L. (2011). Scientific peer review. *Annual Review of Information Science and Technology*, *45*(1), 197–245. https://doi.org/10.1002/aris.2011.1440450112

Bornmann, L., & Mutz, R. (2015). Growth rates of modern science: A bibliometric analysis based on the number of publications and cited references. *Journal of the Association for Information Science and Technology*, *66*(11), 2215–2222. https://doi.org/10.1002/asi.23329

Bray, T. (2017). The JavaScript Object Notation (JSON) Data Interchange Format. https://doi.org/10.17487/RFC8259

Breuning, M., Backstrom, J., Brannon, J., Gross, B. I., & Widmeier, M. (2015). Reviewer fatigue? why scholars decline to review their peers' work. *PS: Political Science & Politics*, *48*(04), 595–600. https://doi.org/10.1017/S1049096515000827

Camenisch, J., Drijvers, M., & Lehmann, A. (2016). Anonymous attestation using the strong diffie hellman assumption revisited. *International Conference on Trust and Trustworthy Computing*, 1–20.

Camenisch, J., & Lysyanskaya, A. (2002). A signature scheme with efficient protocols. *International Conference on Security in Communication Networks*, 268–289.

Cameron, K., Posch, R., & Rannenberg, K. (2009). Appendix d. proposal for a common identity framework: A user-centric identity metasystem. *The Future of Identity in the Information Society*, 477.

Cantor, M., & Gero, S. (2015). The missing metric: Quantifying contributions of reviewers. *Royal Society open science*, *2*(2), 140540. https://doi.org/10.1098/rsos.140540

Chadwick, D., Longley, D., Sporny, M., Terbu, O., Zagidulin, D., & Zundel, B. (2019). Verifiable credentials implementation guidelines 1.0. https://www.w3.org/TR/vc-imp-guide/

Chadwick, D. W., Laborde, R., Oglaza, A., Venant, R., Wazan, S., & Nijjar, M. (2019). Improved identity management with verifiable credentials and fido. *IEEE Communications Standards Magazine*, *3*(4), 14–20. https://doi.org/10.1109/MCOMSTD.001.1900020

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly*, *13*(3), 319. https://doi.org/10.2307/249008

Davis, F. D., Bagozzi, R. P., & Warshaw, P. R. (1989). User acceptance of computer technology: A comparison of two theoretical models. *Management Science*, *35*(8), 982–1003. http://www.jstor.org/stable/2632151

Demir, S. B. (2018). Predatory journals: Who publishes in them and why? *Journal of Informetrics*, *12*(4), 1296–1311.

Derraik, J. G. B. (2015). The principles of fair allocation of peer-review: How much should a researcher be expected to contribute? *Science and Engineering Ethics*, *21*(4), 825–828. https://doi.org/10.1007/s11948-014-9584-2

Di Francesco Maesa, D., & Mori, P. (2020). Blockchain 3.0 applications survey. *Journal of Parallel and Distributed Computing*, *138*, 99–114. https://doi.org/10.1016/j.jpdc.2019.12.019

Dürst, M. J., & Suignard, M. (2005). Internationalized Resource Identifiers (IRIs). https://doi.org/10.17487/RFC3987

E. Ben Sasson, A. Chiesa, C. Garman, M. Green, I. Miers, E. Tromer, & M. Virza. (2016). Zerocash: Decentralized anonymous payments from bitcoin. *2016 IEEE Symposium on Security and Privacy (SP)*, 459–474. https://doi.org/10.1109/SP.2014.36

EU. (2016). Regulation (eu) 2016/679 of the european parliament and of the council of 27 april 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing directive 95/46/ec (general data protection regulation). https://eur-lex.europa.eu/eli/reg/2016/679/oj

Fecher, B., & Friesike, S. (2013). *Open science: One term, five schools of thought*. https://doi.org/10.2139/ssrn.2272036

Ferreira, C., Bastille-Rousseau, G., Bennett, A. M., Ellington, E. H., Terwissen, C., Austin, C., Borlestean, A., Boudreau, M. R., Chan, K., Forsythe, A., Hossie, T. J., Landolt, K., Longhi, J., Otis, J.-A., Peers, M. J. L., Rae, J., Seguin, J., Watt, C., Wehtje, M., & Murray, D. L. (2016). The evolution of peer review as a basis for scientific publication: Directional selection towards a robust discipline? *Biological Reviews*, *91*(3), 597–610. https://doi.org/10.1111/brv.12185

Fox, C. W., Albert, A. Y. K., & Vines, T. H. (2017). Recruitment of reviewers is becoming harder at some journals: A test of the influence of reviewer fatigue at six journals in ecology and evolution. *Research Integrity and Peer Review*, *2*(1), 3. https://doi.org/10.1186/s41073-017-0027-x

Fox, J., & Petchey, O. L. (2010). Pubcreds: Fixing the peer review process by "privatizing" the reviewer commons. *Bulletin of the Ecological Society of America*, *91*(3), 325–333. https://doi.org/10.1890/0012-9623-91.3.325

Fred D. Davis. (1985). *A technology acceptance model for empirically testing new end-user information systems*. https://www.researchgate.net/publication/35465050_A_Technology_Acceptance_Model_for_Empirically_Testing_New_End-User_Information_Systems

Fyfe, A., Coate, K., Curry, S., Lawson, S., Moxham, N., & Røstvik, C. M. (2017). *Untangling academic publishing: A history of the relationship between commercial interests, academic prestige and the circulation of research*. Zenodo. https://doi.org/10.5281/zenodo.546100

Gasparyan, A. Y., Gerasimov, A. N., Voronov, A. A., & Kitas, G. D. (2015). Rewarding peer reviewers: Maintaining the integrity of science communication. *Journal of Korean medical science*, *30*(4), 360–364. https://doi.org/10.3346/jkms.2015.30.4.360

Goldreich, O., Micali, S., & Wigderson, A. (1991). Proofs that yield nothing but their validity or all languages in np have zero-knowledge proof systems. *Journal of the ACM*, *38*(3), 690–728. https://doi.org/10.1145/116825.116852

Goldwasser, S., Micali, S., & Rackoff, C. (1985). The knowledge complexity of interactive proof-systems. In R. Sedgewick (Ed.), *Theory of computing* (pp. 291–304). ACM Press. https://doi.org/10.1145/22145.22178

Grainger, D. W. (2007). Peer review as professional responsibility: A quality control system only as good as the participants. *Biomaterials*, *28*(34), 5199–5203. https://doi.org/10.1016/j.biomaterials.2007.07.004

Green, M. (2017). Zero knowledge proofs: An illustrated primer, part 2. https://blog.cryptographyengineering.com/2017/01/21/zero-knowledge-proofs-an-illustrated-primer-part-2/

Groth, J. (2010). Short pairing-based non-interactive zero-knowledge arguments. In M. Abe (Ed.), *Advances in cryptology - asiacrypt 2010* (pp. 321–340). Springer Berlin Heidelberg.

Hammer-Lahav, E., & Nottingham, M. (2010). Defining Well-Known Uniform Resource Identifiers (URIs). https://doi.org/10.17487/RFC5785

Hauser, M., & Fehr, E. (2007). An incentive solution to the peer review problem. *PLoS biology*, *5*(4), e107. https://doi.org/10.1371/journal.pbio.0050107

Helmy, N. (8 May 2020). A solution for privacy-preserving verifiable credentials. *MATTR*. https://medium.com/mattr-global/a-solution-for-privacy-preserving-verifiable-credentials-f1650aa16093

Hitchens, R. (2018). Selective disclosure in solidity for ethereum - rob hitchens - medium. *Rob Hitchens*. https://medium.com/robhitchens/selective-disclosure-with-proof-f6a1ac7be978

Hochberg, M. E., Chase, J. M., Gotelli, N. J., Hastings, A., & Naeem, S. (2009). The tragedy of the reviewer commons. *Ecology Letters*, *12*(1), 2–4. https://doi.org/10.1111/j.1461-0248.2008.01276.x

Horbach, S. P. J. M., & Halffman, W. (2017). Promoting virtue or punishing fraud: Mapping contrasts in the language of ’scientific integrity’. *Science and Engineering Ethics*, *23*(6), 1461–1485. https://doi.org/10.1007/s11948-016-9858-y

Horbach, S. P. J. M., & Halffman, W. (2018). The changing forms and expectations of peer review. Retrieved, from https://researchintegrityjournal.biomedcentral.com/articles/10.1186/s41073-018-0051-5

Jan, Z., Third, A., Ibanez, L.-D., Bachler, M., Simperl, E., & Domingue, J. (2018). Sciencemiles digital currency for researchers: Companion of the world wide web conference www2018 : April 23-27, 2018, lyon, france. *Companion of the The Web Conference 2018 on The Web Conference 2018 - WWW '18*. https://doi.org/10.1145/3184558.3191556

Janowicz, K., Regalia, B., Hitzler, P., Mai, G., Delbecque, S., Fröhlich, M., Martinent, P., & Lazarus, T. (2018). On the prospects of blockchain and distributed ledger technologies for open science and academic publishing. *Semantic Web*, *9*(5), 545–555. https://doi.org/10.3233/SW-180322

Johnson, D., Menezes, A., & Vanstone, S. (2001). The elliptic curve digital signature algorithm (ecdsa). *International journal of information security*, *1*(1), 36–63.

Jones, M., Bradley, J., & Sakimura, N. (2015). JSON Web Token (JWT). https://doi.org/10.17487/RFC7519

Josefsson, S., & Liusvaara, I. (2017). Edwards-Curve Digital Signature Algorithm (EdDSA). https://doi.org/10.17487/RFC8032

Kachewar, S. G., & Sankaye, S. B. (2013). Reviewer index: A new proposal of rewarding the reviewer. *Mens Sana Monographs*, *11*(1), 274–284. https://doi.org/10.4103/0973-1229.109347

Kondova, G., & Erbguth, J. (2020). Self-sovereign identity on public blockchains and the gdpr. *Proceedings of the 35th Annual ACM Symposium on Applied Computing*, 342–345. https://doi.org/10.1145/3341105.3374066

Kovanis, M., Porcher, R., Ravaud, P., & Trinquart, L. (2016). The global burden of journal peer review in the biomedical literature: Strong imbalance in the collective enterprise. *PLOS ONE*, *11*(11), e0166387. https://doi.org/10.1371/journal.pone.0166387

Langheinrich, M. (2001). Privacy by design — principles of privacy-aware ubiquitous systems. *Ubicomp 2001: Ubiquitous Computing*, 273–291. https://doi.org/10.1007/3-540-45427-6_23

Larivière, V., Haustein, S., & Mongeon, P. (2015). The oligopoly of academic publishers in the digital era. *PLOS ONE*, *10*(6), e0127502. https://doi.org/10.1371/journal.pone.0127502

Lee, C. J., Sugimoto, C. R., Zhang, G., & Cronin, B. (2013). Bias in peer review. *Journal of the American Society for Information Science and Technology*, *64*(1), 2–17. https://doi.org/10.1002/asi.22784

Lodder, M. (2019). Anoncreds 1.0 2.0 update [Accessed on 29.08.2021]. https://docs.google.com/presentation/d/1JRzlzS3Y3NTm_NPzxlnud7xIDmGL_9aHHX55MMwvtlU

Lodder, M., & Looker, T. (2020). Bbs+ signature scheme. https://mattrglobal.github.io/bbs-signatures-spec/

Longley, D., & Sporny, M. (2021). Linked data proofs 1.0. https://w3c-ccg.github.io/ld-proofs/#introduction

Longley, D., Zagidulin, D., & Sporny, M. (2021). The did:key method v0.7. https://w3c-ccg.github.io/did-method-key/

Looker, T., & Steele, O. (2021). Bbs+ signatures 2020. https://w3c-ccg.github.io/ldp-bbs2020/#normative-references

Mahoney, M. J. (1977). Publication prejudices: An experimental study of confirmatory bias in the peer review system. *Cognitive Therapy and Research*, *1*(2), 161–175. https://doi.org/10.1007/BF01173636

Marangunić, N., & Granić, A. (2015). Technology acceptance model: A literature review from 1986 to 2013. *Universal Access in the Information Society*, *14*(1), 81–95. https://doi.org/10.1007/s10209-014-0348-1

MATTR. (2021). Mattrglobal/bbs-signatures: An implementation of bbs+ signatures for node and browser environments [Accessed on 04.09.2021]. https://github.com/mattrglobal/bbs-signatures#element-size

Mayden, K. D. (2012). Peer review: Publication's gold standard. *Journal of the Advanced Practitioner in Oncology*, *3*(2), 117–122.

Mealling, M. H., & Denenberg, R. (2002). Report from the Joint W3C/IETF URI Planning Interest Group: Uniform Resource Identifiers (URIs), URLs, and Uniform Resource Names (URNs): Clarifications and Recommendations. https://doi.org/10.17487/RFC3305

Moxham, N., & Fyfe, A. (2018). The royal society and the prehistory of peer review, 1665–1965. *The Historical Journal*, *61*(4), 863–889. https://doi.org/10.1017/S0018246X17000334

Mulligan, A., Hall, L., & Raphael, E. (2013). Peer review in a changing world: An international study measuring the attitudes of researchers. *Journal of the American Society for Information Science and Technology*, *64*(1), 132–161. https://doi.org/10.1002/asi.22798

Ortega, J. L. (2017). Are peer-review activities related to reviewer bibliometric performance? a scientometric analysis of publons. *Scientometrics*, *112*(2), 947–962. https://doi.org/10.1007/s11192-017-2399-6

Ortega, J. L. (2019). Exploratory analysis of publons metrics and their relationship with bibliometric and altmetric impact. *Aslib Journal of Information Management*, *71*(1), 124–136. https://doi.org/10.1108/AJIM-06-2018-0153

Peffers, K., Tuunanen, T., Rothenberger, M. A., & Chatterjee, S. (2007). A design science research methodology for information systems research. *Journal of Management Information Systems*, *24*(3), 45–77. www.jstor.org/stable/40398896

Perlman, R. (1999). An overview of pki trust models. *IEEE Network*, *13*(6), 38–43. https://doi.org/10.1109/65.806987

Petchey, O. L., Fox, J. W., & Haddon, L. (2014). Imbalance in individual researcher's peer review activities quantified for four british ecological society journals, 2003-2010. *PLOS ONE*, *9*(3), e92896. https://doi.org/10.1371/journal.pone.0092896

Peters, D. P., & Ceci, S. J. (1982). Peer-review practices of psychological journals: The fate of published articles, submitted again. *Behavioral and Brain Sciences*, *5*(2), 187–195. https://doi.org/10.1017/S0140525X00011183

Piwowar, H., Priem, J., Larivière, V., Alperin, J. P., Matthias, L., Norlander, B., Farley, A., West, J., & Haustein, S. (2018). The state of oa: A large-scale analysis of the prevalence and impact of open access articles. *PeerJ*, *6*, e4375. https://doi.org/10.7717/peerj.4375

Pontika, N., Knoth, P., Cancellieri, M., & Pearce, S. (2015). Fostering open science to research using a taxonomy and an elearning portal. In S. Lindstaedt (Ed.), *Proceedings of the 15th international conference on knowledge technologies and data-driven business* (pp. 1–8). ACM. https://doi.org/10.1145/2809563.2809571

Prüfer, J., & Zetland, D. (2010). An auction market for journal articles. *Public Choice*, *145*(3-4), 379–403. https://doi.org/10.1007/s11127-009-9571-3

Publons. (2014). Publons. https://web.archive.org/web/20210414004129/https://publons.com/about/terms/

Publons. (2018). Global state of peer review. https://publons.com/community/gspr

Publons. (2020). Publons. https://web.archive.org/web/20201109015743/https://publons.com/about/home

Qi, X., Deng, H., & Guo, X. (2017). Characteristics of retractions related to faked peer reviews: An overview. *Postgraduate medical journal*, *93*(1102), 499–503. https://doi.org/10.1136/postgradmedj-2016-133969

R. Mukta, J. Martens, H. -y. Paik, Q. Lu, & S. S. Kanhere. (2020). Blockchain-based verifiable credential sharing with selective disclosure. *2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, 959–966. https://doi.org/10.1109/TrustCom50675.2020.00128

Raoult, V. (2020). How many papers should scientists be reviewing? an analysis using verified peer review reports. *Publications*, *8*(1), 4. https://doi.org/10.3390/publications8010004

Rawat, S., & Meena, S. (2014). Publish or perish: Where are we heading? *Journal of Research in Medical Sciences : The Official Journal of Isfahan University of Medical Sciences*, *19*(2), 87–89.

Reed, D., Sporny, M., Longley, D., Allen, C., Grant, R., & Sabadello, M. (2021). Decentralized identifiers (dids) v1.0. https://www.w3.org/TR/did-core/

Rescorla, E. (2018). The Transport Layer Security (TLS) Protocol Version 1.3. https://doi.org/10.17487/RFC8446

RetractionWatch. (2015). https://web.archive.org/web/20210224101355/https://retractionwatch.com/2015/08/17/64-more-papers-retracted-for-fake-reviews-this-time-from-springer-journals/

Rivest, R. L., Shamir, A., & Adleman, L. (1978). A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, *21*(2), 120–126.

Rose, D. M. T., Hollenbeck, S., & Masinter, L. M. (2003). Guidelines for the Use of Extensible Markup Language (XML) within IETF Protocols. https://doi.org/10.17487/RFC3470

Ross-Hellauer, T. (2017). What is open peer review? a systematic review. *F1000Research*, *6*, 588. https://doi.org/10.12688/f1000research.11369.2

Ross-Hellauer, T., Deppe, A., & Schmidt, B. (2017). Survey on open peer review: Attitudes and experience amongst editors, authors and reviewers. *PLOS ONE*, *12*(12), e0189311. https://doi.org/10.1371/journal.pone.0189311

Rossner, M., van Epps, H., & Hill, E. (2007). Show me the data. *Journal of Cell Biology*, *179*(6), 1091–1092. https://doi.org/10.1083/jcb.200711140

Rothwell, P. M., & Martyn, C. N. (2000). Reproducibility of peer review in clinical neuroscience. is agreement between reviewers any greater than would be expected by chance alone? *Brain : a journal of neurology*, *123 (Pt 9)*, 1964–1969. https://doi.org/10.1093/brain/123.9.1964

Sakemi, Y., Kobayashi, T., Saito, T., & Wahby, R. S. (2020). *Pairing-Friendly Curves* (Internet-Draft draft-irtf-cfrg-pairing-friendly-curves-09) [Work in Progress]. Internet Engineering Task Force. Internet Engineering Task Force. https://datatracker.ietf.org/doc/html/draft-irtf-cfrg-pairing-friendly-curves-09

Schroter, S., Black, N., Evans, S., Carpenter, J., Godlee, F., & Smith, R. (2004). Effects of training on quality of peer review: Randomised controlled trial. *BMJ*, *328*(7441), 673. https://doi.org/10.1136/bmj.38023.700775.AE

Smith, D. R. (2015). Will publons popularize the scientific peer-review process? https://doi.org/10.1038/nature.2015.17204

Smith, R. (2006). Peer review: A flawed process at the heart of science and journals. *Journal of the Royal Society of Medicine*, *99*(4), 178–182. https://doi.org/10.1258/jrsm.99.4.178

Spearpoint, M. (2017). A proposed currency system for academic peer review payments using the blockchain technology. *Publications*, *5*(3), 19. https://doi.org/10.3390/publications5030019

Sporny, M., Longley, D., & Chadwick, D. W. (2019). Verifiable credentials data model 1.0. Retrieved December 5, 2020, from https://www.w3.org/TR/vc-data-model/#what-is-a-verifiable-credential

Sporny, M., Longley, D., Kellogg, G., Landthaler, M., Champin, P.-A., & Lindström, N. (2020). Json-ld 1.1. https://www.w3.org/TR/json-ld11/

Squazzoni, F., Bravo, G., & Takács, K. (2013). Does incentive provision increase the quality of peer review? an experimental study. *Research Policy*, *42*(1), 287–294. https://doi.org/10.1016/j.respol.2012.04.014

Steele, O., & Sporny, M. (2021). Did specification registries. https://www.w3.org/TR/did-spec-registries/#did-methods

Supak Smolcić, V. (2013). Salami publication: Definitions and examples. *Biochemia Medica*, *23*(3), 237–241. https://doi.org/10.11613/BM.2013.030

Tarkhanov, I. A., Fomin–Nilov, D. V., & Fomin, M. V. (2020). Crypto access: Is it possible to use cryptocurrencies in scholarly periodicals? *Learned Publishing*. https://doi.org/10.1002/leap.1331

Taylor & Francis. (2015). Peer review in 2015: A global view.

Teixeira da Silva, J. A. (2013). *The thomson reuters impact factor: Critical questions that scientists should be asking* (Vol. 7). https://www.researchgate.net/publication/283719293_The_Thomson_Reuters_Impact_Factor_Critical_Questions_that_Scientists_Should_be_Asking

Teixeira da Silva, J. A. (2017). Fake peer reviews, fake identities, fake accounts, fake data: Beware! *AME Medical Journal*, *2*, 28. https://doi.org/10.21037/amj.2017.02.10

Teixeira da Silva, J. A. (2020). Are negative reviews, predatory reviewers or failed peer review rewarded at publons? *International Orthopaedics*, 1–2. https://doi.org/10.1007/s00264-020-04587-w

Teixeira da Silva, J. A., & Al-Khatib, A. (2019). The clarivate tm analytics acquisition of publons – an evolution or commodification of peer review? *Research Ethics*, *15*(3-4), 1–11. https://doi.org/10.1177/1747016117739941

Tennant, J. (2018). *Democratising knowledge: A report on the scholarly publisher, elsevier*. Zenodo. https://doi.org/10.5281/zenodo.1744583

Tennant, J. (2020). *Time to stop the exploitation of free academic labour*. https://doi.org/10.31235/osf.io/6quxg

Tennant, J. P. (2018). The state of the art in peer review. *FEMS Microbiology Letters*, *365*(19). https://doi.org/10.1093/femsle/fny204

Tennant, J. P., Dugan, J. M., Graziotin, D., Jacques, D. C., Waldner, F., Mietchen, D., Elkhatib, Y., B Collister, L., Pikas, C. K., Crick, T., Masuzzo, P., Caravaggi, A., Berg, D. R., Niemeyer, K. E., Ross-Hellauer, T., Mannheimer, S., Rigling, L., Katz, D. S., Greshake Tzovaras, B., … Colomb, J. (2017). A multi-disciplinary perspective on emergent and future innovations in peer review. *F1000Research*, *6*, 1151. https://doi.org/10.12688/f1000research.12037.3

Tennant, J. P., & Ross-Hellauer, T. (2020). The limitations to our understanding of peer review. Retrieved, from https://researchintegrityjournal.biomedcentral.com/articles/10.1186/s41073-020-00092-1

Tenorio-Fornés, A., Jacynycz, V., Llop-Vila, D., Sánchez-Ruiz, A., & Hassan, S. (2019). Towards a decentralized process for scientific publication and peer review using blockchain and ipfs. In T. Bui (Ed.), *Proceedings of the 52nd hawaii international conference on system sciences*. Hawaii International Conference on System Sciences. https://doi.org/10.24251/HICSS.2019.560

Therese, A. (2018). What's new with peer review on orcid. https://web.archive.org/web/20210120074219/https://info.orcid.org/whats-new-with-peer-review-on-orcid/

Tite, L., & Schroter, S. (2007). Why do peer reviewers decline to review? a survey. *Journal of Epidemiology and Community Health*, *61*(1), 9–12. https://doi.org/10.1136/jech.2006.049817

Trovò, B., & Massari, N. (2021). Ants-review: A privacy-oriented protocol for incentivized open peer reviews on ethereum. In B. Balis, D. B. Heras, L. Antonelli, A. Bracciali, T. Gruber, J. Hyun-Wook, M. Kuhn, S. L. Scott, D. Unat, & R. Wyrzykowski (Eds.), *Euro-par 2020: Parallel processing workshops* (pp. 18–29). Springer International Publishing.

van Bokkem, D., Hageman, R., Koning, G., Nguyen, L., & Zarin, N. (n.d.). Self-sovereign identity solutions: The necessity of blockchain technology. https://arxiv.org/pdf/1904.12816

van Rooyen, S., Godlee, F., Evans, S., Black, N., & Smith, R. (1999). Effect of open peer review on quality of reviews and on reviewers' recommendations: A randomised trial. *BMJ*, *318*(7175), 23–27. https://doi.org/10.1136/bmj.318.7175.23

Veríssimo, D., & Roberts, D. L. (2013). The academic welfare state: Making peer-review count. *Trends in Ecology & Evolution*, *28*(11), 623–624. https://doi.org/10.1016/j.tree.2013.07.003

Vicente-Saez, R., & Martinez-Fuentes, C. (2018). Open science now: A systematic literature review for an integrated definition. *Journal of Business Research*, *88*, 428–436. https://doi.org/10.1016/j.jbusres.2017.12.043

Ware, M. (2008). Peer review in scholarly journals: Perspective of the scholarly community - an international study. https://www.researchgate.net/publication/237295758_

Peer_Review_in_Scholarly_Journals_Perspective_of_the_Scholarly_Community_-_an_International_Study

Ware, M., & Mabe, M. (2015). *The stm report: An overview of scientific and scholarly journal publishing*. https://www.researchgate.net/publication/298355459_The_STM_Report_An_overview_of_scientific_and_scholarly_journal_publishing

Warne, V. (2016). Rewarding reviewers - sense or sensibility? a wiley study explained. *Learned Publishing*, *29*(1), 41–50. https://doi.org/10.1002/leap.1002

Willis, M. (2016). Why do peer reviewers decline to review manuscripts? a study of reviewer invitation responses. *Learned Publishing*, *29*(1), 5–7. https://doi.org/10.1002/leap.1006

Wilson, P. (2020). Academic fraud. *Exchanges: The Interdisciplinary Research Journal*, *7*(3), 14–44. https://doi.org/10.31273/eirj.v7i3.546

Wolfram, D., Wang, P., Hembree, A., & Park, H. (2020). Open peer review: Promoting transparency in open science. Retrieved, from https://link.springer.com/article/10.1007%2Fs11192-020-03488-4#citeas

Xia, J., Harmon, J. L., Connolly, K. G., Donnelly, R. M., Anderson, M. R., & Howard, H. A. (2015). Who publishes in "predatory" journals? *Journal of the Association for Information Science and Technology*, *66*(7), 1406–1417.

Young, K. (2021). *Verifiable credentials flavors explained*. https://www.lfph.io/wp-content/uploads/2021/02/Verifiable-Credentials-Flavors-Explained.pdf

Young, S. N. (2003). Peer review of manuscripts: Theory and practice. *Journal of Psychiatry and Neuroscience*, *28*(5), 327–330.

Zuckerman, H., & Merton, R. K. (1971). Patterns of evaluation in science: Institutionalisation, structure and functions of the referee system. *Minerva*, *9*(1), 66–100. https://doi.org/10.1007/BF01553188