Preprint from: https://www.gipp.com/pub/
Cite: B. Gipp, C. Breitinger, N. Meuschke, J. Beel, "CryptSubmit: Introducing Securely Timestamped Manuscript Submission and Peer Review Feedback using the Blockchain," in *Proceedings of the ACM/IEEE-CS Joint Conference on Digital Libraries (JCDL)*, Toronto, Canada, 2017.

CryptSubmit: Introducing Securely Timestamped Manuscript Submission and Peer Review Feedback using the Blockchain

Bela Gipp[1] Corinna Breitinger[1] Norman Meuschke[1] Joeran Beel

Department of Computer and Information Science
University of Konstanz

[1]{first.last}@uni-konstanz.de

School of Computer Science
& Statistics / ADAPT Centre
Trinity College Dublin

joeran.beel@adaptcentre.ie

ABSTRACT
Manuscript submission systems are a central fixture in scholarly publishing. However, researchers who submit their unpublished work to a conference or journal must trust that the system and its provider will not accidentally or willfully leak unpublished findings. Additionally, researchers must trust that the program committee and the anonymous peer reviewers will not plagiarize unpublished ideas or results. To address these weaknesses, we propose a method that automatically creates a publicly verifiable, tamper-proof timestamp for manuscripts utilizing the decentralized Bitcoin blockchain. The presented method hashes each submitted manuscript and uses the API of the timestamping service OriginStamp to persistently embed this manuscript hash on Bitcoin's blockchain. Researchers can use this tamper-proof trusted timestamp to prove that their manuscript existed in its specific form at the time of submission to a conference or journal. This verifiability allows researchers to stake a claim to their research findings and intellectual property, even in the face of vulnerable submission platforms or dishonest peer reviewers. Optionally, the system also associates trusted timestamps with the feedback and ideas shared by peer reviewers to increase the traceability of ideas. The proposed concept, which we introduce as CryptSubmit, is currently being integrated into the open-source conference management system OJS. In the future, the method could be integrated at nearly no overhead cost into other manuscript submission systems, such as EasyChair, ConfTool, or Ambra. The introduced method can also improve electronic pre-print services and storage systems for research data.

CCS Concepts
H.3.4 [**Information Storage and Retrieval**]: Systems and Software

Keywords
Electronic publishing; peer review; manuscript submission; blockchain; conference management; scientific data management.

1. INTRODUCTION
Manuscript submission systems have become the standard in scholarly publishing. These systems help organizers of academic conferences and journals coordinate all stages of the publishing process: from abstract and manuscript submission, to organizing peer review, and finally receiving camera-ready manuscripts. Manuscript submission systems have significantly reduced the receipt-to-acceptance wait time, thus benefiting organizers and researchers alike [13]. Although manuscript submission systems have made the peer review process more efficient, technical weaknesses of the systems and potential dishonesty of individuals involved continue to threaten the integrity of the process.

A technical limitation is the lack of standards for the secure architecture of manuscript submission systems. To give one example, from 2004 – 2011, Sheridan Printing's conference management software, which was used by many ACM conferences, including WWW and SIGCHI, featured an easily guessable naming scheme for all paper submissions [14]. This naming scheme enabled anyone with the base URL to systematically retrieve all papers submitted to a particular conference. A dishonest individual could have downloaded troves of yet unpublished research papers months before their publication. Such a breach could result in the premature publishing of valuable results, the plagiarism of ideas, or even the loss of pending patent applications if the description of an idea is made openly available on the Web. Researchers have described improved security features, such as a system, for which undesired data flow was precluded through extensive formal verification of the system [8]. However, even ensuring that the data within a manuscript submission system is only visible to the desired parties does not eliminate all weaknesses of such systems.

An inherent human-related challenge to the manuscript submission and peer-review process is its susceptibility to bias and fraud. For example, some reviewers may criticize a submitted manuscript more harshly than justified with the aim of delaying the publication of a competing research group. In extreme cases, peer reviewers, chairs, or editors may even reject a manuscript only to use valuable findings in their own research or publication. While such behavior is likely rare, several cases have been publicized in which peer reviewers plagiarized ideas and results from the unpublished manuscripts that they were entrusted with reviewing [2, 4, 11, 12]. Recently, a medical researcher discovered that five years' worth of research data from his lab, on the relationship between lipoprotein levels and diet had been plagiarized in a journal article. It turned out that the plagiarist had been a peer reviewer for a prestigious medical journal, for which he had read and rejected the original authors' manuscript before publishing the research results as if they were his own [3]. Such examples of academic misconduct remind us that entrusting

JCDL'17, June 19–23, 2017, Toronto, Ontario, Canada.

anonymous reviewers with novel research results via a black-box manuscript submission system poses a risk to researchers.

The problem of academic plagiarism is as old as academia itself [9]. The development and use of more sophisticated automated plagiarism detection software can only increase the effort required to plagiarize, but will not eliminate the problem [6]. Therefore, ensuring the verifiability of one's own research contributions is a valuable precaution to defend against potential plagiarism.

However, currently researchers are missing a method to securely and effortlessly prove their academic contributions in the face of potential data leakage or fraud. The question arises:

How can researchers prove that their contribution already existed at the time of submission to a conference or journal?

In this paper, we propose a method that enables any researcher to securely verify the existence of research ideas, data, or results at the time of a manuscript's submission. The method generates a hash, i.e. a unique fingerprint, of the research manuscript and accompanying data, which is embedded in the tamper-proof blockchain of the cryptocurrency Bitcoin. Using this approach, the manuscript is associated with a permanent and inalterable trusted timestamp that is publicly verifiable. If the content of a manuscript is misappropriated later, the trusted timestamp lets the author prove, independently of the manuscript submission system, that a manuscript already existed in a precise state at the time it was submitted to a conference or journal.

2. BACKGROUND

We briefly present some state-of-the-art manuscript submission systems and describe their limitations.

2.1 Existing Systems

Systems to support the academic publishing process can be broadly categorized into electronic publishing systems, also referred to as journal management systems, and conference management systems. Both system types support the peer-review process from accepting authors' manuscript submissions, over selecting reviewers and managing their feedback, to accepting the final manuscript and formatting it for publication. Conference management systems typically provide additional functionality, such as registration and payment handling, event organization including the scheduling of sessions, rooms, and speakers, and the ability to publish conference information on the Web. Since our presented approach addresses the peer-review process, this section examines both types of systems, as long as they offer a peer-review functionality.

A large number and variety of manuscript submission systems are available. Editorial Manager[1] by Aries Systems is the most widely-used commercial journal management system. Publishers, such as Springer Nature, BMC and PLOS, employ this mature and feature-rich system to manage thousands of journals. Among academic conference management systems, EasyChair[2] and ConfTool[3] are widely-used solutions. Both systems follow a freemium business model, i.e., vendors provide free licenses for a basic version of the systems, but require payment for more advanced features. The code of the systems cannot be hosted on one's own server and is not open source. A review of additional systems can be found in [10].

In the following, we focus on popular *open-source* systems, since these give us the opportunity to instantaneously integrate the capability of trusted timestamping.

Ambra[4] is a mature Java-based journal management system maintained by the Public Library of Science (PLOS). The first version of Ambra was released in 2007; before the code was developed as part of the PLOS Topaz project. Ambra is employed by several PLOS journals, including PLOS ONE. The PHP-based Open Journal System (OJS)[5] is an alternative to Ambra with comparable features and degree of maturity. The application is developed by the Public Knowledge Project and was first released in 2001. This organization also maintains the Open Conference Systems (OCS)[6] software for conference management. HotCRP[7] is an alternative open-source conference management system introduced in 2006 and used by several ACM SIG conferences. OJS, OCS and HotCRP offer the option of using a hosted instance of the systems for a fee. Deploying the systems on one's own server is free of charge, as is the case for Ambra.

In summary, although there are many manuscript submission systems to choose from, they share the same shortcoming: they provide no evidence or mechanism to verifiably prove the content of a submitted manuscript. The most evidence provided by existing submission systems is a confirmation email that the systems send out to acknowledge the successful reception of the manuscript. Sometimes these emails also attach the abstract or manuscript submitted. However, the reliability and persistency of such evidence is not guaranteed. The verifiability of the content of confirmation emails depends on the availability of a corresponding data record on the side of the publisher to whom the manuscript was submitted. This record can easily go missing, e.g. due to limited retention periods for such data, because the manuscript submission system changes, or because the publisher ceases to exist. The data record of the manuscript submission system may also be manipulated, e.g., by malicious conference organizers or editors who plan to plagiarize from submitted work.

No currently available manuscript submission system offers authors a mechanism to obtain a tamper-proof and persistent piece of evidence that is independent of the system itself and enables authors to verifiably prove that they submitted a research work at a specific time.

3. SYSTEM CONCEPT

Having described the limitations of existing manuscript submission systems, we present the concept and prototype, *CryptSubmit*, which we implemented into the open source system OJS. CryptSubmit uses the Bitcoin blockchain to enable tamperproof, decentralized timestamping of all data exchanged during the manuscript submission and peer review process. Section 3.1 describes the blockchain-based approach to timestamping and our service OriginStamp, which CryptSubmit uses to generate trusted timestamps. Section 3.2 presents details on CryptSubmit.

[1] http://www.ariessys.com/software/editorial-manager
[2] http://easychair.org/users.cgi
[3] http://www.conftool.net
[4] http://www.ambraproject.org
[5] https://pkp.sfu.ca/ojs/
[6] https://pkp.sfu.ca/ocs/
[7] http://www.read.seas.harvard.edu/~kohler/hotcrp

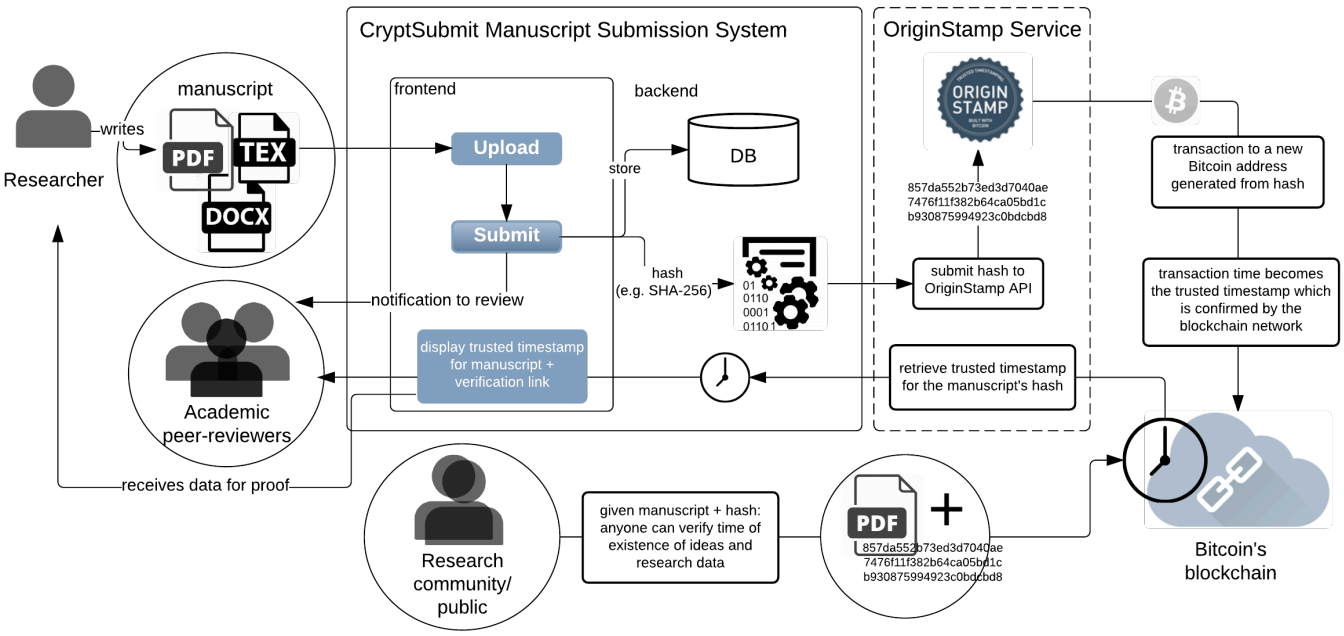

Figure 1: Overview of CryptSubmit as implemented in OJS.

3.1 Trusted Timestamping on the Blockchain

We introduced decentralized trusted timestamping of digital files using the blockchain of a cryptocurrency as the medium for timestamp generation and verification in [5]. With OriginStamp[8], we provide a non-commercial, web-based service for creating decentralized trusted timestamps on Bitcoin's blockchain.

The idea of decentralized trusted timestamping is to permanently embed a hash, i.e. a unique fingerprint, of a digital file in the distributed blockchain of a cryptocurrency. The implementation of the approach in OriginStamp computes a SHA-256 hash of the file to be timestamped using Java Script running in the user's web browser. Computing the hash in the browser ensures the raw data does not leave the user's machine. To provide the service free of charge, OriginStamp keeps the transaction costs in the blockchain to a minimum by collecting all hashes received over a 24-hour period and computing a single aggregate SHA-256 hash from the list of hashes. We employ Base58 encoding to transform the aggregate hash into a string that conforms to the requirements for a valid Bitcoin address. Since the aggregate hash is unique, so is the resulting Bitcoin address. We then trigger a Bitcoin transaction that transfers the smallest possible transaction amount (1 Satoshi) to the newly created, unique address. Since the address identifies the aggregate hash and each Bitcoin transaction is assigned a timestamp, both the content and its time of existence is stored and cryptographically secured in the blockchain. As soon as the block that includes the transaction is formed (average duration of 10 minutes) and confirmed, the transaction is permanently embedded in all copies of the decentralized blockchain. Users receive all data needed to verify the inclusion of their hashes in the blockchain even if OriginStamp would no longer be available. One option for verifying the existence of a particular transaction is to use one of the many visual blockchain explorers, such as blockexplorer.com or blockchain.info. Alternatively, users can directly search within a copy of the blockchain.

The benefit of the blockchain-based approach, compared to traditional digital timestamping [1, 7], is the independence of a central timestamping authority (TSA). In traditional digital timestamping, a TSA issues the timestamps and verifies their validity. This approach requires trust in the integrity of the TSA, and ties the verifiability of timestamps to the availability of the TSA. If the TSA is compromised, e.g. due to technical errors or malicious activity, timestamps could be altered. If the TSA becomes unavailable, timestamps are no longer verifiable. In decentralized trusted timestamping, the cryptographic security of blockchains replaces the need for trust in a TSA. The created timestamp is secure as long as the cryptographic methods are secure. The timestamp is guaranteed to be verifiable as long as a single copy of the blockchain exists. Since the blockchain is redundantly stored on thousands of computing nodes, the persistency of the timestamp is virtually guaranteed.

3.2 CryptSubmit

Figure 1 illustrates the architecture of the CryptSubmit system. The system's frontend provides standard functionality for user registration, manuscript upload and submission, as well as for the organization of the peer review process. As soon as a registered researcher submits a manuscript file, and optionally accompanying material, such as images, videos, or data files, the system's backend immediately hashes the submitted files and sends their hash via POST request to the OriginStamp API. Once the hash of the submitted files has been embedded in the blockchain, the manuscript's authors receive a zip-archive containing the submitted files together with the other hashes included in the Bitcoin transaction. Zipping the files prevents accidental alterations to the files. Additionally, the timestamp and a confirmation link are displayed in the system frontend.

Reviewers provide their feedback using online forms following the established process of manuscript submission systems. In contrast to existing systems, CryptSubmit uses the OriginStamp API to timestamp each submitted review both with and without including identifying information of reviewers, such as name,

[8] www.originstamp.org. Before registering originstamp.org, the service was available at http://gipp.com/originstamp since 2012.

email, affiliation, and an ORCID[9] if provided by the reviewer. The timestamp for the anonymous version of the form is provided to the authors of the reviewed manuscript. The other timestamp is send to the reviewer and available in the reviewer and organizer view of the system. Since the timestamp is verifiable independent of the CryptSubmit system, authors can give credit to reviewers, e.g., for providing valuable ideas, by citing the transaction that records the feedback in the Bitcoin blockchain. CryptSubmit allows authors to request lifting the anonymity of reviewers to enable personalized citations for received feedback. If the organizers and the reviewers agree to the request, the authors are granted access to the review form that includes the reviewer's details and its corresponding timestamp.

Augmenting a manuscript submission system with decentralized trusted timestamping has several benefits. First, authors receive a cryptographically secured timestamp for their research manuscript as it existed, bit-exact, at the time of submission. The persistence and verifiability of this timestamp is independent of the submission platform. If data or results are leaked or redistributed prior to publication in the intended channel, researchers can use the timestamp to support their claim to research contributions.

Second, the approach can deter potential plagiarists since all individuals involved in the manuscript submission and peer review process, e.g., program committee members or reviewers, know that a manuscript's existence is permanently verifiable.

Third, reviewers receive an additional incentive to provide valuable feedback, since they receive a proof of existence for their input and can allow authors to cite their contributions.

We are currently integrating the proposed concept into the open-source manuscript submission system OJS. We are also in contact with EasyChair and other leading providers of commercial manuscript submission systems. After the completion in spring 2017, we will make the source code openly available to encourage other developers to integrate decentralized trusted timestamping into their own conference management systems.

4. CONCLUSION & FUTURE WORK

We introduced an approach for securely timestamping manuscripts and reviewer feedback submitted in manuscript submission systems using the Bitcoin blockchain. This procedure allows the authors and the public to independently verify that a manuscript, a dataset, or other research results already existed in a precise format at the time of submission to a conference or journal. Researchers must not place their trust in the security or the existence of the submission platform itself to verify the time at which a manuscript was submitted to a conference or journal. Plagiarism of yet unpublished research results due to leaks, or peer reviewer dishonesty, can more easily be proven by the original author.

The proposed approach could equally benefit other submission systems, e.g. for research grant proposals, or university applications. The approach can also be integrated into open science repositories, such as Harvard's Dataverse[10], where researchers can upload their datasets, or into online pre-print repositories, such as arXiv.org[11].

The idea of embedding data in a cryptographically secured blockchain could be expanded to the point where the full texts of the manuscripts are openly stored on a blockchain ledger. Existing pre-print services, typically maintained by a single provider, could be replaced with a decentralized open access pre-print service that leverages a blockchain to transparently store files and verifiably track all changes performed on those files. The blockchain could for instance be maintained by a network of research institutions, government agencies, and other organizations.

This manuscript has been timestamped on the Blockchain and is verifiable under: http://www.originstamp.org/u/3q7vJLZS2h

5. REFERENCES

[1] Adams, C. and Pinkas, D. 2001. Internet X. 509 public key infrastructure time-stamp protocol (TSP).

[2] Cantrill, S. 2016. "I am really sorry:" Peer reviewer stole text for own paper. *Retraction Watch*.

[3] Dansinger, M. 2016. Dear Plagiarist: A Letter to a Peer Reviewer Who Stole and Published Our Manuscript as His Own. *Annals of Internal Medicine*.

[4] Degen, R. 2016. Peer reviewer steals text for his own chemistry paper, gets sanctioned by journal. *Retraction Watch*.

[5] Gipp, B. et al. 2015. Decentralized Trusted Timestamping using the Crypto Currency Bitcoin. *Proceedings of the iConference 2015* (Newport Beach, California, Mar. 2015).

[6] Gipp, B. et al. 2014. Web-based Demonstration of Semantic Similarity Detection Using Citation Pattern Visualization for a Cross Language Plagiarism Case. *Special Session on Information Systems Security within Proceedings of the 16th International Conference on Enterprise Information Systems (ICEIS)* (Lisbon, Portugal, 2014), 677–683.

[7] Haber, S. and Stornetta, W.S. 1991. How to Time-Stamp a Digital Document. *Advances in Cryptology—CRYPTO '90 Proceedings*. 3, 2, 99–111.

[8] Kanav, S. et al. 2014. A conference management system with verified document confidentiality. *Intl. Conference on Computer Aided Verification* (2014), 167–183.

[9] Meuschke, N. and Gipp, B. 2013. State-of-the-art in detecting academic plagiarism. *International Journal for Educational Integrity*. 9, 1.

[10] Parra, L. et al. 2013. Comparison of online platforms for the review process of conference papers. *The Fifth International Conference on Creative Content Technologies*, 16–22.

[11] Sticklen, M.B. 2010. Retraction Notice: Plant genetic engineering for biofuel production: towards affordable cellulosic ethanol. *Nature Reviews Genetics*. 11, 4, 308.

[12] University of Waterloo suspends researcher who published plagiarized paper — in his own journal: 2013. *http://retractionwatch.com/2013/01/08/university-of-waterloo-suspends-researcher-who-published-plagiarized-paper-in-his-own-journal/*.

[13] Ware, M. 2005. Online submission and peer-review systems. *Learned publishing*. 18, 4, 245–250.

[14] Wimmer, R. 2011. Why you should not trust Sheridan Printing with your conference paper.

[9] https://orcid.org
[10] http://dataverse.org
[11] http://arxiv.org