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

ADAPT Centre
Trinity College Dublin

[1]{first.last}@uni-konstanz.de joeran.beel@adaptcentre.ie

ABSTRACT

Manuscript submission systems are a central fixture in scholarly publishing. However, with existing systems, researchers must trust that their yet unpublished findings will not prematurely be disseminated due to technical weaknesses and that anonymous peer reviewers or committee members will not plagiarize unpublished content. To address this limitation, we present CryptSubmit – a system that automatically creates a decentralized, tamperproof, and publicly verifiable timestamp for each submitted manuscript by utilizing the blockchain of the cryptocurrency Bitcoin. The publicly accessible and tamperproof infrastructure of the blockchain allows researchers to independently verify the validity of the timestamp associated with their manuscript at the time of submission to a conference or journal. Our system supports researchers in protecting their intellectual property even in the face of vulnerable submission platforms or dishonest peer reviewers. Optionally, the system also generates trusted timestamps for the feedback shared by peer reviewers to increase the traceability of ideas. CryptSubmit integrates these features 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 a standard tool 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 [16]. Although manuscript submission systems have made peer review more efficient, technical weaknesses and potential dishonesty of the involved individuals threaten the integrity of the scientific peer review process.

A first weakness, of technical nature, 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 paper submissions [17]. This weakness enabled anyone with the base URL to systematically retrieve all papers submitted to a conference months before their publication. Such data leaks from submission platforms can lead to the premature release of results, the plagiarism of ideas, or even the loss of potential patent applications if the description of an idea is made openly available on the Web.

A further weakness, this time of human nature, is the risk of bias or fraud in the peer-review process. Some reviewers may criticize a submitted manuscript more harshly than justified with the aim of delaying competing researchers. In extreme cases, peer reviewers, chairs, or editors may reject a manuscript only to use its valuable findings in their own research and publication. Such unethical behavior is likely rare. However, several cases have been publicized in which peer reviewers plagiarized ideas and results from the unpublished manuscripts they reviewed [3, 5, 14, 15]. Only recently, a medical researcher discovered that five years' worth of his lab's data had been plagiarized and published. The plagiarist had received access to this data while acting as a peer reviewer for a prestigious medical journal, where he had rejected the original manuscript before publishing the data as if it was his own [4]. Such severe cases of academic misconduct remind us that entrusting anonymous reviewers with novel research results via a submission system poses a risk for plagiarism.

While the problem of academic plagiarism is as old as academia itself [12] and can never be entirely eliminated, the development and use of more sophisticated plagiarism detection systems can help examiners to more quickly discover the extent of plagiarism, as well as to increase the effort plagiarists must put forth to avoid detection [6, 11]. We expect that having a means to securely verify priority for research manuscripts upon their submission represents one additional deterrence against academic plagiarism.

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

978-1-5386-3861-3/17/$31.00 ©2017 IEEE

The question arises:

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

In this paper, we propose a method which enables researchers to securely verify the existence of research ideas, data, or results at the time of a manuscript's submission for review. The proposed method generates a hash, i.e. a unique fingerprint, of the research manuscript and accompanying data, if included. The hash is embedded in the tamperproof blockchain of the cryptocurrency Bitcoin, however, any blockchain, e.g. Ethereum, could equally be used for this purpose. This approach, coined in a previous paper as decentralized trusted timestamping [7], associates a digital file with a tamperproof timestamp recorded on the blockchain that is permanently and publicly verifiable. If a manuscript's content is misappropriated later, the trusted timestamp allows the author to prove that the manuscript already existed in a precise state when it was submitted to a conference or journal – fully independent of the manuscript submission system used.

2. EXISTING SYSTEMS

While several applications exist that exploit Bitcoin's blockchain for trusted-timestamping [2, 9], no system exists that utilizes the blockchain with the objective of enabling researchers to document priority for their academic manuscripts.

Today's systems supporting the academic publishing process can be categorized into electronic publishing systems, also referred to as journal management systems, and conference management systems. Both types of systems support the peer-review process: from accepting manuscript submissions, over selecting reviewers and managing their feedback, to accepting the final manuscript and formatting it for publication. Conference management systems typically include event organization functionalities, as well as registration and payment handling. Since our presented approach addresses the peer-review process, we examine both system types, as long as they offer a peer-review functionality.

Editorial Manager[1] by Aries Systems is a 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., offering a free basic version, while requiring payment for more advanced features. The code of the systems is not open source and cannot be hosted on one's own server. A review of additional systems can be found in [13].

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) and employed by several PLOS journals. The PHP-based Open Journal System (OJS)[5] offers comparable features and degree of maturity as Ambra. OJS is developed by the Public Knowledge Project, which also maintains the Open Conference Systems (OCS)[6] software for conference management. HotCRP[7] is an alternative open-source conference management system 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.

While openly available manuscript submission systems exist, they share the same shortcoming: they provide authors with no mechanism to obtain a persistent piece of evidence that is independent of the system itself and enables authors to verifiably prove that a research work was submitted at a given time. The most evidence provided by existing systems is a confirmation email to acknowledge the receipt of the manuscript. However, 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 may also be manipulated, e.g., by malicious conference organizers or editors who plan to plagiarize from submitted work.

3. SYSTEM CONCEPT

Having described the limitations of existing manuscript submission systems, we present the concept and prototype, *CryptSubmit*[8], which we implemented into the open-source manuscript submission system OJS. CryptSubmit uses the blockchain of Bitcoin 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.

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 [7]. With OriginStamp[9], 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 JavaScript 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 minimizes the transaction costs (currently approx. 9 cents per Bitcoin transaction), by collecting all hashes received over a 24-hour period and computing a single aggregate SHA-256 hash from all submitted hashes. OriginStamp then employs Base58 encoding to transform this aggregate hash into a string that conforms to the requirements for a valid Bitcoin address [7]. Since the aggregate hash is unique, so is the resulting Bitcoin address. OriginStamp triggers a transaction to this address to which it transfers the smallest unit of Bitcoin, i.e. 1 Satoshi.

[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
[8] available for testing from: https://www.gipp.com/cryptsubmit/
[9] www.originstamp.org. Before registering originstamp.org, the service was available at http://gipp.com/originstamp since 2012.

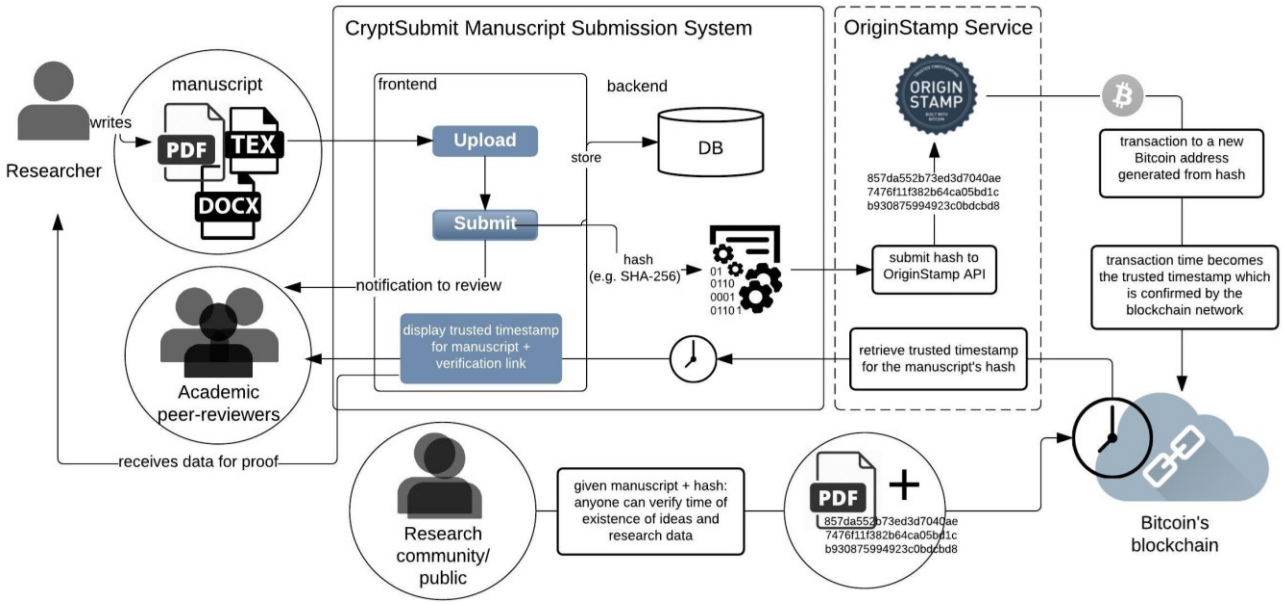

Figure 1: Overview of CryptSubmit as implemented in OJS.

At today's Bitcoin value, 1 Satoshi is equivalent to 0.00001 USD, so this cost is negligible in comparison to the previously mentioned transaction fee. Since the Bitcoin address derives from the aggregate hash and each Bitcoin transaction is assigned a timestamp, both a representation of the content and its time of existence are stored and cryptographically secured in the blockchain. As soon as the block containing that transaction is formed and confirmed (average duration of 10 minutes), the transaction will be permanently embedded in all copies of the decentralized blockchain.

The benefit of the blockchain-based approach, compared to traditional digital timestamping [1, 10], 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 timestamps are secure as long as the cryptographic mechanisms of the blockchain are secure.

3.2 CryptSubmit

Figure 1 shows the architecture of the CryptSubmit system. The system's frontend provides standard functionality for user registration, manuscript upload as well as for the organization of the peer review process. When authors submit their manuscript, and optionally supplementary 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. Zipping the files prevents accidental alterations to the files. Additionally, the timestamp and a confirmation link are displayed in the system frontend.

The authors also receive a confirmation email with all data needed to verify the inclusion of their hash(es) in the blockchain even if the CryptSubmit manuscript submission platform would no longer exist. One option for verifying the existence and time of a 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 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.

Reviewers give feedback using an online form following the same process as in currently existing manuscript submission systems. In contrast to existing systems, CryptSubmit timestamps each submitted review – once with and once without the identifying information of reviewers, e.g., name, email, affiliation, and an ORCID[10] if provided. The timestamp of the anonymous version of the form is provided to the authors of the reviewed manuscript. The other timestamp is sent to the reviewer and is visible in the reviewer and organizer view of the system. Since all timestamps are 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 blockchain. CryptSubmit allows authors to request lifting the anonymity of reviewers to allow citing the received feedback. If the reviewers agree to the request, the authors are granted access to the review form with the reviewer's details and its corresponding timestamp.

Augmenting a manuscript submission system with decentralized trusted timestamping results in several improvements. First, authors receive a tamperproof 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 integrity of the submission platform. If data or results are leaked prior to publication in the intended venue, researchers can use the timestamp to support their claim to research contributions.

Second, the approach may deter plagiarists, since all individuals involved in the manuscript submission and peer review process, e.g. program committee members and reviewers, are aware that a manuscript's time of existence is permanently verifiable. The idea

[10] https://orcid.org

of CryptSubmit is not to prevent academic plagiarism, but rather to help authors prove their intellectual property and to support examiners in more easily confirming the existence of plagiarism, which is also a goal of plagiarism detection and visualization tools [6]. Just as existing automated plagiarism detection systems can only deter potential plagiarists [8], CryptSubmit will not prevent academic plagiarism, but its capability may deter some plagiarists.

Finally, reviewers could be incentivized to more openly share their own ideas, since they receive a proof of existence for their feedback and can allow authors to cite their contributions.

We have integrated the proposed concept into the open-source manuscript submission system OJS as a proof-of concept, and made the code available under a GNU General Public License to encourage other developers to integrate decentralized trusted timestamping into their own conference management systems. Currently, we are in contact with leading providers of manuscript submission systems to explore the possibility of integrating trusted timestamping into an established system.

4. CONCLUSION & FUTURE WORK

We introduced an approach for securely timestamping manuscripts and reviewer feedback submitted in manuscript submission systems using Bitcoin's 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. As a result, 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[11], where researchers can upload their datasets, or into online pre-print repositories, such as arXiv.org[12].

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. ACKNOWLEDGEMENTS

This research has benefited from the support of the Carl Zeiss Foundation and the Science Foundation Ireland (SFI) under Grant Number 13/RC/2106.

6. REFERENCES

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

[2] Breitinger, C. and Gipp, B. 2017. VirtualPatent - Enabling the Traceability of Ideas Shared Online using Decentralized Trusted Timestamping. *Proceedings of the 15th Int. Symposium of Information Science* (2017).

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

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

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

[6] Gipp, B. et al. 2014. Citation-based Plagiarism Detection: Practicability on a Large-scale Scientific Corpus. *Journal of the American Society for Information Science and Technology (JASIST)*. 65, 2 (2014), 1527–1540.

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

[8] Gipp, B. et al. 2013. Demonstration of citation pattern analysis for plagiarism detection. *Proceedings of the 36th Int. ACM SIGIR conference on Research and development in information retrieval - SIGIR '13* (New York, New York, USA, 2013), 1119.

[9] Gipp, B. et al. 2016. Securing Video Integrity Using Decentralized Trusted Timestamping on the Blockchain. *10th Mediterranean Conference on Information Systems (MCIS)* (Lisbon, Portugal, Apr. 2016), 3–17.

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

[11] Meuschke, N. and Gipp, B. 2014. Reducing computational effort for plagiarism detection by using citation characteristics to limit retrieval space. *Proceedings of the 14th ACM/IEEE-CS Joint Conference on Digital Libraries* (2014), 197–200.

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

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

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

[15] 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/*.

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

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

[11] http://dataverse.org

[12] http://arxiv.org