Thomas Hepp*, Alexander Schoenhals, Christopher Gondek, and Bela Gipp

OriginStamp: A blockchain-backed system for decentralized trusted timestamping

Abstract: Currently, timestamps are certified by central timestamping authorities, which have disadvantages of centralization. The concept of the decentralized trusted timestamping (DTT) was developed by Gipp et al. to address these drawbacks. The paper provides insights into the architecture and implementation of a decentralized timestamp service taking the integration of multiple blockchain types into account. Furthermore, the components are introduced and the versatile application scenarios are presented. A future direction of research is the evaluation of blockchain technology and their suitability for timestamping.

Keywords: Decentralized Trusted Timestamping, Blockchain Technology, Blockchain Systems, Distributed Ledger Technology

ACM CCS: Security and privacy → Security services → Privacy-preserving protocols

1 Introduction

The proof of existence is more important than ever before. This is about the proof that content exists at a certain point in time. On the one hand, more and more processes are being digitized, accelerating our businesses and life. On the other hand, the progressive digitization increases the possibility of manipulation. The race between encryption and decryption technologies is gaining momentum [17]. More and more complex encryption methods are being developed, which suspects try to circumvent. To change the author of a decrypted document, just a few clicks are usu-

*Corresponding author: Thomas Hepp, Universität Konstanz, Information Science Group, D-78464 Konstanz, Germany, e-mail: thomas.hepp@uni-konstanz.de, ORCID: http://orcid.org/0000-0002-7671-0602
Alexander Schoenhals, University of Konstanz, Information Science Group, D-78464 Konstanz, Germany, e-mail: alexander.schoenhals@uni-konstanz.de
Christopher Gondek, Bela Gipp, Universität Konstanz, Information Science Group, D-78464 Konstanz, Germany, e-mails: christopher.gondek@uni-konstanz.de, bela.gipp@uni-konstanz.de

ally sufficient. In the event of copyright infringement, the existence of a document must be proven beyond doubt for the author to receive his or her attribution. Timestamping plays an important role in different business processes, e. g., copyright of intellectual property or in future patent litigation to prove who had an idea first. Images and videos are often not recognized in courts as evidence of the possibility of manipulation [9]. Therefore, a method is required to timestamp digital content. In the past, central services were used for this purpose. The users have to trust this central instance and are therefore directly dependent on their security to be protected against manipulation. The blockchain as part of the peer-to-peer electronic cash system by Nakamoto was introduced in 2008 [19] and is regarded as a tamper-proof, decentralized data structure. The characteristics of blockchain technology are perfectly suited to address this challenge. The following paper deals with the technical solution of this problem. How can the blockchain technology be integrated into an application to generate and verify timestamps of any digital content?

In Section 2 the current state of the art is examined, which methods are available for timestamping and what the strengths and weaknesses of these techniques are. The approach for timestamping on the Bitcoin blockchain is proposed in Section 3. Moreover, the components which are essential for the timestamping are explained in detail. Our technical solution is presented in Section 4. There we describe the individual modules and their interaction in more detail. At the end of this work in Section 5, we present the conclusions of our solution and give an outlook on future research.

2 Background

The idea of verifiable timestamps in the digital world is not new. Before the digital era, even post stamps were used as timestamps to prove the existence of documents. To protect a novel discovery, inventors in the 18th century sent letters to themselves and collected them in a safe.

Traditional methods, such as public notaries, are not applicable for the increasing digitization of the everyday life. The most important aspect is the rapidly increasing amount of digital content.

Due to copyright restrictions, we cannot publish the full text of this article on our website

To receive a **pre-print of the full text**, please send an email to:
thomas.hepp@uni-konstanz.de

To obtain the **published version**, please visit the publisher's
website: https://doi.org/10.1515/itit-2018-0020

Citation data for this article

[1] T. Hepp et al. "OriginStamp: A blockchain-backed system for decentralized trusted timestamping". In: *it - Information Technology* (Nov. 2018). DOI: 10.1515/itit-2018-0020.

Listing 1: Use the following BibTeX code to cite this article

```
@article{Hepp2018c,
  doi = {10.1515/itit-2018-0020},
  url = {https://doi.org/10.1515/itit-2018-0020},
  year  = {2018},
  month = {nov},
  publisher = {Walter de Gruyter {GmbH}},
  author = {Thomas Hepp and Alexander Schoenhals and
      Christopher Gondek and Bela Gipp},
  title = {{OriginStamp}: A blockchain-backed system for
      decentralized trusted timestamping},
  journal = {it - Information Technology}
}
```