Proceedings of the 8th European Conference on Social Media

UCLan Cyprus

Larnaca, Cyprus

1-2 July 2021

Edited by

Dr Christos Karpasitis

A conference managed by ACI, UK

Proceedings of the

8th European Conference on Social Media

ECSM 2021

A Virtual Conference

Hosted By

University of Central Lancaster, UCLan Cyprus

1-2 July 2021

Review Process
Papers submitted to this conference have been double-blind peer reviewed before final acceptance to the conference. Initially, abstracts were reviewed for relevance and accessibility and successful authors were invited to submit full papers. Many thanks to the reviewers who helped ensure the quality of all the submissions.

Ethics and Publication Malpractice Policy
ACPIL adheres to a strict ethics and publication malpractice policy for all publications – details of which can be found here:
http://www.academic-conferences.org/policies/ethics-policy-for-publishing-in-the-conference-proceedings-of-academic-conferences-and-publishing-international-limited/

Self-Archiving and Paper Repositories
We actively encourage authors of papers in ACPIL conference proceedings and journals to upload their published papers to university repositories and research bodies such as ResearchGate and Academic.edu. Full reference to the original publication should be provided.

Conference Proceedings
The Conference Proceedings is a book published with an ISBN and ISSN. The proceedings have been submitted to a number of accreditation, citation and indexing bodies including Thomson ISI Web of Science and Elsevier Scopus.

Author affiliation details in these proceedings have been reproduced as supplied by the authors themselves.

The Electronic version of the Conference Proceedings is available to download from DROPBOX **https://tinyurl.com/ECSM21** Select Download and then Direct Download to access the Pdf file. Free download is available for conference participants for a period of 2 weeks after the conference.

The Conference Proceedings for this year and previous years can be purchased from http://academic-bookshop.com

E-Book ISBN: 978-1-914587-01-6
E-Book ISSN: 2055-7221
Book version ISBN: 978-1-912764-63-1
Book Version ISSN: 2055-7213

Published by Academic Conferences International Limited
Reading, UK
+44 (0) 118 324 6938www.academic-conferences.org
info@academic-conferences.org

On the use of Blockchain Technologies and Digital Identity to Safeguard and Verify the Integrity of Source Material

Alexander Pfeiffer[1, 2, 3], Stephen Bezzina[2, 3] and Thomas Wernbacher[1]
[1]Donau-Universität Krems (DUK), Krems, Austria
[2]University of Malta (UM), Msida, Malta
[3]B&P Emerging Technologies Consultancy Lab Ltd, St. Julians, Malta
Alexander.pfeiffer@donau-uni.ac.at
mail@stephenbezzina.com
Thomas.wernbacher@donau-uni.ac.at
DOI: 10.34190/ESM.21.018

Abstract: In addition to the general intentional scattering of fake news and its conscious or unconscious sharing on social media networks, the problem of checking the origin of source material from the perspective of the consumer is evident. This is especially the case if the original material was not created and registered with great care by established and trustworthy media companies. In the fast-paced world of real-time reporting, even professional media houses have to rely on cell phone videos or other user-created material. Furthermore, it is also possible that source material only appears to have been produced by an established media company, but instead journalists who work with this material fall victim to well-crafted forgery. The aim of this research study is to discuss Blockchain technologies and their adoption to store a verification hash of source material, the proof of authorship and sources used in a forgery-proof way. Furthermore, the authors investigate whether journalists and media producers see a need in this technology. The discussion centres around the consumers' perception of such possible verification as an improvement and something they recognize as a "trust amplifier" if embedded in the newspaper, journal, blog, social media platform, or messenger tool of their choice. Finally, the sociological and ethical dimensions are briefly discussed - whether and how verified material can ultimately be fake news once again, and if the perception of what one believes, does not depend at the end on the recipient's basic attitude and perception. This work in progress paper describes the current status of the research work and outlines the envisaged further procedure.

Keywords: Blockchain, DLT, Social Media, Journalism, Fake News

1. Introduction

For Grech and Camilleri (2017), the authors of the "JRC Science for Policy Report: Blockchain in Education", Blockchain offers significant opportunities, particularly from a socioeconomic perspective, that go beyond the current ways in which we deal with data storage. In particular, the transfer of data sets into the Blockchain and the rapid verification of their validity opens new possibilities in the future. According to Grech and Camilleri, Blockchain offers:

- "Self-sovereignty, i.e., for users to identify themselves while at the same time maintaining control over the storage and management of their personal data;
- Trust, i.e., for a technical infrastructure that gives people enough confidence in its operations to carry through with transactions such as payments or the issue of certificates;
- Transparency & Provenance, i.e., for users to conduct transactions in knowledge that each party has the capacity to enter into that transaction;
- Immutability, i.e., for records to be written and stored permanently, without the possibility of modification;
- Disintermediation, i.e., the removal of the need for a central controlling authority to manage transactions or keep records;
- Collaboration, i.e., the ability of parties to transact directly with each other without the need for mediating third parties. (p. 8)

In this work in progress paper, the authors discuss the topic of Blockchain technologies in the context of securing digital material related to content production, source of origin, and the identity of its creators. To develop a theoretical basis, the authors conducted an intensive literature review on the topics of fake news and its scientific analysis from various points of view. The basic literature presented in this paper is mostly from current work in Behavioral Cybersecurity: Fundamental Principles and Applications of Personality Psychology by Patterson and Winston-Proctor (2020). Among other things, the topics of fake news based on political communication (since 2016) are dealt with in this book. Furthermore, current events in the Covid-19 crisis and cryptography are addressed in this publication. Also, and highly relevant to the purpose of this paper, is the work

on 'Fake News' in The International Encyclopaedia of Media Psychology (Tandoc, Chew & Lim, 2020). The authors see fake news as a type of disinformation that derives its power to mislead from mimicking the look and feel of real news. The authors suggest that the public is routinely exposed to different types of fake news online, from sites pretending to be news platforms, to social media and even messaging apps. Grazulis and Rogers (2021) discuss the effect of describing someone else's coverage as Fake News, especially to discredit this information in advance among their own supporters. In this context, Grazulis and Rogers refer for example to the Trump administration. Dordevic, Pourghomi and Safieddine identitfied in their paper "Identifying Fake News from the Variables that Governs the Spread of Fake News" (2020) a total of twenty-seven variables around this topic from different perspectives, like the recipient, content posted on social media, and metrics from social media analysis. Dordevic et al. identified key factors like mismatching of time and mention of Artificial Intelligence (AI) as a possible solution to cross-reference data and prevent fake news. However, the authors do not address the issue of Blockchain and identity. The basic work of Dovdevic et al. is an excellent basis for our project. And our work could be seen as an optimal complement and extension to their original research question[1].

In relation to Blockchain technologies and social media, the use of Blockchain technologies to protect the ownership and/or the author has been addressed by Cai et. al. (2018), while the adoption of Blockchain to prevent spreading rumours has been researched by Chen et. al. (2018). Blockchain technologies and their use to prove that any media has a non-manipulated original has been described by Bhowmik and Feng (2017). This provides a solid basis for further consideration by the authors of this work, the planned prototype, and the basis for the expert discussions. In this context, other relevant work conducted by Hasan and Salah (2019), discusses how Blockchain can protect users from deep-fakes. Stjernfelt and Lauritzen (2020) present work on how to safeguard freedom of speech through decentralised server infrastructure, while Unger et. al. (2015) look into secure and encrypt peer2peer messages. The Whitepaper of the Sovrin Foundation (2017) addresses the important topic of digital identity and log in management using self-sovereign identity (SSI) on Blockchain. Lastly, Pfeiffer et. al. provided an overview of different social networks and how they embedded Blockchain as technology (2020).

2. Presentation of the developed demonstrator

For this paper, we have developed a demonstrator, realized on the testnet of the proof-of-stake Blockchain Ardor (childchain Ignis)[2]. Within the framework of a fictitious case study, roles are distributed and typical actions of all involved institutes and persons are acted out. These case studies will be conducted in three iterations. The results of the third iteration will be prepared for the experts and presented during the expert panel.

The three key roles that Blockchain addresses are assigned to are:

- A journalism club, which serves as an official registry for journalists in a country. A structure that already exists in many countries.
- A fictitious publishing and media house.
- Three different roles of media professionals; a self-employed author, a freelancer, and a fixed employee in the above-mentioned media house.

The role play will cover the process of publishing the Blockchain address of the journalism club in an official government journal, its own website, and as a message to its own address on the Blockchain. It will also cater for the registration of members of the journalism club using Blockchain-based utility tokens generated for this purpose on the testnet. These journalism club members can be private individuals on the one hand and legal entities (such as the publishing and media company) on the other.

From the point of view of the media company, it will be shown how their fixed employees and their freelancers are registered. On the one hand, the linking of persons already registered in the journalism club and, on the other hand, registration in the club through the publisher's register will be demonstrated and discussed. This also addresses the respective permissions for exercising tasks, digital identities, and timestamps. It will be shown how the digital proof of authorship can be used for online articles, in social media channels, but also in offline articles, for example with printed articles in the respective magazine and on the Blockchain registered

[1] What are the key variables in the spread of fake news? Can the understanding of these variables support an approach to automate the detection of fake news?
[2] See https://www.jelurida.com

identification codes. In addition to linking to articles and authorship, it will also point out how authors can register source material on the Blockchain using their digital identity.

Finally, the demonstration features how readers can now verify the respective information using tools such as a block explorer. The risk that a complete infrastructure could be faked, meaning that a fake block explorer is generated to create fake news, will also be debated.

3. Planned research aims and methods used

An online survey administrated amongst media professionals and consumers will be chosen by the authors as a data collection tool, followed by an expert discussion in which the results of both questionnaires will be discussed. Furthermore, the authors debate with the experts the demonstrator described above, with the aim of showing how Blockchain and digital identity can be combined to represent the chain-of-trust of source material. The expert interviews will then be evaluated following the qualitative content analysis according to Mayring (2010).

Finally, the sociological and ethical dimensions will be briefly discussed - whether and how verified material can ultimately be fake news once again, and if the perception of what one believes, does not depend at the end on the recipient's basic attitude and perception.

This results in the following research questions for the planned final paper:

- What is the possible impact of the use of Blockchain technologies and digital identity to safeguard and verify the integrity of source material from the publisher's as well as the recipient's perspective?
- To what extent can Blockchain and digital identities limit the spread of fake news?
- To what extent can digital proof of identity on a Blockchain basis harm authors and their sources?
- To what extent can digital proof of identity on a Blockchain basis be used to deliberately give fake news a certain amount of additional power in regards to the degree of make believe for the targeted recipients?
- How can Blockchain-based digital proof of identity be set up so that readers develop a natural understanding of it and how to use the tools?

4. Conclusion

The innovation of the finished paper will be a sound example of how the chain of trust in content creation is mapped on Blockchain. This case study is discussed with the experts from different points of view incorporated with insights from the relevant literature. Through this approach, the authors hope to provide a new foundation for further research projects in the field of Blockchain, journalism, and content creation in traditional media, but especially in social networks.

Acknowledgements

We would like to thank Alesha Serada for the critical discussion on our research topic and their constant and true remark that recipients often do not want to check sources and like to simply believe content, especially if it agrees with their basic beliefs.

References

Bhowmik, D. and Feng, T. (2017) The multimedia Blockchain: A distributed and tamper-proof media transaction framework 22nd International Conference on Digital Signal Processing (DSP), London, 2017, pp. 1-5.

Cai, W., Wang, Z., Ernst, J. B., Hong, Z., Feng C. and Leung V. C. M. (2018) Decentralized Applications: The Blockchain-Empowered Software System in IEEE Access, vol. 6, pp. 530 19-53033

Chen, Y., Li, Q and Wang, H. (2018) Towards Trusted Social Networks with Blockchain Technology, Paper accepted to Symposium on Foundations and Applications of Blockchain 2018 (FAB '18), arXiv:1801.02796v2

Dordevic, M.; Pourghomi P.; Safieddine, F. (2020) "Identifying Fake News from the Variables that Governs the Spread of Fake News.," 2020 15th International Workshop on Semantic and Social Media Adaptation and Personalization (SMA, Zakynthos, Greece, 2020, pp. 1-6, doi: 10.1109/SMAP49528.2020.9248453.

Grazulis, A., & Rogers, R. (2021). "Ridiculous and Untrue – FAKE NEWS!": The Impact of Labeling Fake News. In Management Association, I. (Ed.), Research Anthology on Fake News, Political Warfare, and Combatting the Spread of Misinformation (pp. 25-38). IGI Global. http://doi:10.4018/978-1-7998-7291-7.ch002

Grech, A. and Camilleri A. (2017) Blockchain in Education. (HRC Science for Policy Report). https://doi.org/10.2760/60649

Hasan, HR and Salah, K (2019) Combating Deepfake Videos Using Blockchain and Smart Contracts in IEEE Access, vol. 7, pp. 41596-41606, doi: 10.1109/ACCESS.2019.2905689

Mayring, P. (2010.) Qualitative Inhaltsanalyse; Grundlagen und Techniken, Beltz Verlag, Weinheim, Basel

Patterson, W., & Winston-Proctor, C.E. (2020). Behavioral Cybersecurity: Fundamental Principles and Applications of Personality Psychology (1st ed.). CRC Press. https://doi.org/10.1201/9781003052029

Pfeiffer, A.; Kriglstein, S.; Wernbacher, T.; Bezzina, S. (2020). Blockchain Technologies and Social Media: A Snapshot. In: Proceedings of the 7th European Conference on Social Media ECSM 2020, 2020: 196, Academic Conferences and Publishing International Limited, Limerick, doi: 10.34190/ESM.20.073

Sovrin Foundation (2017) The Inevitable Rise of Self-Sovereign, A white paper from the Sovrin Foundation, edited by Andrew Tobin & Drummond Reed

Stjernfelt, F. and Lauritzen, A. M. (2020) Your Post has been Removed, Springer Open, Cham Switzerland, https://doi.org/10.1007/978-3-030-25968-6

Tandoc, E.C., Jr., Chew, M. and Lim, D. (2020). Fake News. In The International Encyclopedia of Media Psychology, J. Bulck (Ed.). https://doi.org/10.1002/9781119011071.iemp0300

Unger, N., Dechand S., Bonneau, J., Fahl, S., Perl, H., Goldberg, I., Smith, M. (2015) SoK: Secure Messaging in 2015 IEEE Symposium on Security and Privacy, San Jose, CA, pp. 232-249. doi: 10.1109/SP.2015.22