BLOCKCHAIN TECHNOLOGIES AS DATA STORAGE FOR TEST RESULTS AND CERTIFICATES - THE HUMAN FACTOR

A. Pfeiffer[1,4,5], S. Kriglstein[2], S. Bezzina[3], N. König[4], T. Wernbacher[4], A. Dingli[5], V. Vella[5]

[1]Massachusetts Institute of Technology (UNITED STATES)
[2]AIT Austrian Institute of Technology GmbH (AUSTRIA)
[3]Ministry for Education and Employment (MALTA)
[4]Donau-University Krems (AUSTRIA)
[5]University of Malta (MALTA)

Abstract

In the educational sector even the most sophisticated digital environments will not make human interaction obsolete, as learning and education are inherently social processes. This also means that any application that involves learning and assessment must deal with problems resulting from human error. Some of these problems can effectively be countered or excluded by Blockchain-based technologies. Especially in the case of retroactive manipulation of data, non-Blockchain systems are prone to manipulation, as even the most advanced safeguards cannot prohibit users with high enough access rights to manipulate existing data entries (this may be a mere annoyance when a well-meaning teacher edits a student's attendance, but it can quickly become a large-scale problem when the recognition of diplomas is tampered with on an institutional level). As data stored on the Blockchain cannot be altered retroactively, the problem of tampering with existing data is to be ruled out.

This conference paper looks at the role of humans in the use of state-of-the-art systems that store grades from exams and certificates on Blockchain, and aims at initiating a broad discussion whilst providing guidance for future developments.

Keywords: Blockchain, Assessment, Errors, Humans.

1 INTRODUCTION

Humans remain a potential source of error, especially in the educational sector, where even the most sophisticated digital environments will not make human interaction obsolete, as learning and education are inherently social processes. This also means that any application that involves learning and assessment must deal with problems caused by human intervention. Some of these problems can effectively be countered or excluded by Blockchain-based technologies. Especially in the case of retroactive manipulation of data, non-Blockchain systems are prone to manipulation, as even the most advanced safeguards cannot prohibit users with high enough access rights to manipulate existing data entries (this may be a mere annoyance when a well-meaning teacher edits a student's attendance, but it can quickly become a large-scale problem when the recognition of diplomas is tampered with on an institutional level). As data stored on the Blockchain cannot be altered retroactively, the problem of tampering with existing data is to be ruled out [1].

However, even when a Blockchain-system secures the storage and management of data, there are still humans involved in the process. Especially when Blockchain is used only for the final storage of grades, there is still plenty of room for error. Imagine the following: students take an exam, the professor tells his assistant to note the grades, which are then dropped off at a secretary's desk, who then emails the grade to the Blockcerts-department[1] of the university to secure the entry on Blockchain. This process offers many opportunities for human error, ranging from unfair grading by the professor and/or his assistant, to the assistant mixing up U.S. and European grading scales, to the secretary mistyping when copying the grade, to the Blockcerts-clerk assigning the grade to the wrong student.

[1] https://www.blockcerts.org/ is an open standard for Blockchain-based credential already implemented at selected schools and universities. It is based on 1-way hash verification. Originally developed to work using the Bitcoin Blockchain.

This problem might be reduced when a holistic learning and assessment system is entirely based on the Blockchain, as this allows to store test results immediately, and to ensure that grades are calculated based on a fixed key and in real time. Consequently, the aim of this paper is to identify problems that can occur when using Blockchain technologies in the educational sector.

2 GROUNDWORK LITERATURE AND RELATED RESEACH

Our desk research has revealed that there is currently no literature on the potential of human errors associated with the use of Blockchain technologies in the educational sector. Publications on the human-side of Blockchain are to be generally considered as very rare. Only the viewpoint of how Blockchain, from a technological perspective, can generate automations and thereby trust is dealt with in most of the recent works on Blockchain which involve a perspective on the role of humans.

This contribution is therefore a first and very early explorative approach.

One of the few articles about Blockchain and the human factor is by Prakhovnik and colleagues. In the article *“The Human Factor In Blockchain Technology”* [2], the authors deal relatively superficially with the problem of private keys and the fact that they cannot be recovered if lost. If there is a possibility of recovery via a central identity, an attack on the key can be carried out. The authors did not look into approaches like using Shamir's Secret Sharing (SSS in short), where a private key is divided into multiple pieces, giving each participant its own shared piece. To combine the original key, a minimum number of pieces is required which is typically less than the total number of pieces. For example any 2 out 3 shared pieces will reproduce the key. Such a technology is for instance already being implemented into the ARDOR Network[2].

Schmidt [3] wrote a valuable fundamental book on Blockchain technologies from different technical but also socially relevant perspectives, such as legislation. The anonymous person Satoshi Nakamoto [4] suggested a currency without centralized trust center based on a Blockchain in his famous whitepaper "Bitcoin: a peer-to-peer electronic cash system" in 2008. This article constitutes for many, the beginning of the use of blockchain technologies as we know them today. Grech and Camilleri [5], in their EU report on Blockchain in Education, provide a fundamental reference document on the use of Blockchain technologies beyond the purpose of cryptocurrencies. In particular, they describe different types of networks, such as private, consortium-led or public Blockchains work. But also, the functionality of Smart Contracts and the concept of Utility Tokens with reference to use cases in the educational sector are discussed. The authors [6] of this paper have surveyed the level of knowledge about Blockchain in the educational sector. One goal was to determine where the hurdles for a successful implementation are. One of the findings is that extensive education and practical training is required.

3 RESEARCH QUESTIONS

This conference contribution will look into the following research question:

- Which kind of errors can occur through human interventions and how can such errors be corrected when Blockchain technologies are used?

4 METHODOLOGY

To achieve their research goal, the authors conducted a focus group discussion with 5 participants. Table 1 details the gender and respective background for each participant. The core question of the discussion equates to the research question presented above. The realization of the focus group is based on the method of the problem-centered interview following Witzel [8], whilst the evaluation of the key statements was conducted according to Mayring's [7] approach in regard to content-analyses.

Note: All participants of the focus group have a good to very good knowledge on the topic of Blockchain technologies.

[2] https://www.jelurida.com is the landing page to learn more about the ARDOR Blockchain System.

Table 1. Participants of the Focus Group

Person	Gender	Background
1	m	Educational sector
2	f	IT sector
3	f	Educational sector
4	m	Sociology
5	m	Economics

5 RESULTS

In the following sections, the authors summarize the core statements of the research question, in the form of a content summary, which is attached to the specific identified problems.

> *"Which kind of errors can occur through human interventions and how can such errors be corrected when Blockchain technologies are used?"*

5.1 Bribing or other reasons to achieve better test results

When grades are awarded, there is always a risk of bribery unless several randomly selected and independent examiners are present and/or fully automated systems with reliable identity verifications are used. The reasons for bribery are many and various. The experts brought several examples that they are familiar from the press, for example the manipulation of SAT scores in America or the manipulated Italian tests of a soccer star in order for him/her to obtain citizenship and not be considered as a foreigner when joining a top club in the country. Background agreements and monetary payments are also very difficult to detect. As long as the identity of the examinee is not clearly verifiable and provable, it is assumed that only this person was sitting in front of the exam PC during the whole process. Otherwise, if the examinee knows exactly who his examiners are, risks related to bribe are possible. In such cases even blockchain cannot help directly, as it needs other systems for support, like webcams or randomized examiner selection. In such cases, the only thing that blockchain can do is to help ensure that the grades are not manipulated afterwards. Since a new data record must be created for each correction, the initiator is always verified and a time stamp (that cannot be falsified) is automatically generated. However, this does not always ensure that it was actually performed by the specific person in case the identity itself was stolen.

5.2 Examinations taken by another person, for example with the help of a Ghost Writer

For written submissions, e.g. in case of conventional homework, the application and adoption of Blockchain technology is limited. In such instances, other technologies such as automated writing style analysis using Artificial Intelligence (AI) are more adequate. However, this requires a huge amount of data material from the student and is very cost and time intensive. The easiest way to counteract this kind of fraud is to still take oral examinations in addition to the written assignments.

5.3 Faulty programming of the Blockchain systems or underlying Smart Contracts

Another aspect is, of course, that during the programming of the Blockchain systems errors can occur, which may not be detected until a few years later and then lead to massive problems. This can happen especially with minor blockchain systems, where the community of reviewers is not big enough to identify such issues. The most frequent errors are human mistakes in the programming of Smart Contracts, often resulting in fatal consequences.

5.4 Identity theft through social engineering or hacks

A big problem, of course, is always related to identity, both from the point of view of the student and from the point of view of the examiner who gives the grades. Identities can either be stolen by technical means, for example by a data leak or through social engineering. In such scenarios, a fraudster obtains sufficient data about a person by interacting with the victim personally and under false pretenses. Of course, the damage can be enormous if, for example, someone obtains the identity of an administrator and fraudulently issues certificates in the name of an institution. Here, blockchain can support red flags which are issued in relation to a certificate number and consequently systems that validate certificates will look for assigned revocation. This implies that a certificate would be invalid from the moment the certificate is blocked.

5.5 Incorrect handling due to lack of knowledge of how Blockchain works and what it implies

A basic problem that has been identified is the frequent lack of knowledge about the basic technology being used and therefore simple mistakes in using it.

5.6 Input errors due to carelessness

Another problem caused by human intervention can result from carelessness, a consequence of overworked staff, underpayment or other personal factors. As a result, data can be entered incorrectly and require subsequent correction. In terms of Blockchain, this requires a new transmission and thus an additional line in the digital examination book of the examinee.

5.7 Insecure forwarding of data via e-mail and manipulation of off-chain systems

Another problem occurs when people use insecure systems to transfer data. For example, someone sends data to another person via unencrypted e-mail, and the recipient then has to enter it into the Blockchain exam tool. Another problem is when the system from which the grade is given and the system on which the grade is saved are not connected.

The participants of the focus group bring the example of a term paper as an examination work. After submission and evaluation by the lecturer, the grade is first saved in Moodle, as sometimes several sub-grades result in an overall grade. At the end of the process, the grade is transferred manually or via insecure systems such as e-mail or FTP to another location where the grades are stored in the university grading system. Here is much room for manipulation.

5.8 Management of Private Keys and the problem of centralized Log-In Systems

Another potential issue is the management of logins to the different accounts. And this concern was the one that triggered the longest discussion within the focus group interviews. In the purist Blockchain community there is the motto: "not your key, not your coins". This refers to the fact that every user has his own private key, which is unrecoverable and therefore has to be kept unique and secure. Criminals can get this key by using the methods described above, but also by using malware like keyloggers. However, in the educational sector, it will probably be not possible to pursue this purist approach. In fact, the consulted experts did not reach a consensus on the way forward. One possibility would be that the keys are managed purely by the Blockchain system and people have no read access to them. This system is connected to the software via a typical user and password system. Another possibility would be that keys are split and there is a recovery fragment, so to speak. This fragment must be in trustworthy hands or an AI-based computer system. In relation to this, an expert refers to the Shamir's Secret Sharing method. As such, key management is and will remain an essential aspect, especially in relation to the role of humans as operators of Blockchain-based grade administration systems.

6 CONCLUSIONS & FUTURE RESEARCH

Based on the extensively discussed aspects, recommendations for action are to be drawn up. Research and development must increasingly focus on the role of humans as an important aspect of Blockchain-based databases. There is a need for more information on which systems exist, showing the possibilities of Blockchain for different sectors, such as Education. Furthermore, the role of human beings as an important aspect of Blockchain-based databases is to be further explored. This includes the investigation of the possibilities brought about by Blockchain for different sectors, like Education, with an objective focus also on the dangers and misuse of this technology.

ACKNOWLEDGEMENTS

The authors thank the participants of the focus group.

REFERENCES

[1] Atzei, N., Bartoletti, M., Lande, S., Zunino, R., A Formal Model of Bitcoin Transactions, in S. Meiklejohn, K. Sako (eds.). Financial Cryptography and Data Security. FC 2018, Lecture Notes in Computer Science, vol. 10957, pp. 551–60, Berlin, Heidelberg., 2018

[2] Prakhovnik, N., Zemlyanska, O., Klushka, M., THE HUMAN FACTOR IN BLOCKCHAIN TECHNOLOGY. 10.36074/22.12.2019.v1.20., 2020

[3] Schmidt, N., Kryptowährungen und Blockchains, in Technologie, Praxis, Recht, Steuern, Linde Verlag, Wien, 2019

[4] Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, in Whitepaper; online available under: https://bitcoin.org/bitcoin.pdf, 2008

[5] Grech, A.; Camilleri, A. F., Blockchain in Education. Luxembourg, in Publications Office of the European Union 2017, 132 S. - (JRC Science for Policy Report) - URN: urn:nbn:de:0111-pedocs-150132, 2017

[6] Pfeiffer, A., Bezzina, S., Wernbacher, T., Kriglstein S., THE ROLE OF BLOCKCHAIN TECHNOLOGIES IN DIGITAL ASSESSMENT, EDULEARN20 Proceedings, pp. 395-403, 10.21125/edulearn.2020.0175, 2020

[7] Mayring, P., Qualitative Inhaltsanalyse; Grundlagen und Techniken, Beltz Verlag, Weinheim, Basel, 2010

[8] Witzel, A.. Das problemzentrierte Interview. In Qualitative Forschung in der Psychologie : Grundfragen, Verfahrensweisen, Anwendungsfelder, Gerd Jüttemann (Ed.). Beltz, Weinheim, 227–255, 1985