Hochschule für Technik
und Wirtschaft Berlin
University of Applied Sciences

Hochschule für Technik
und Wirtschaft Berlin
University of Applied Sciences

Proceedings of the
19th European Conference on e-Learning
A Virtual Conference hosted by University of Applied Sciences HTW Berlin, Germany
28-30 October 2020

Edited by
Prof. Dr.-Ing. Carsten Busch, Martin Steinicke and Prof. Dr. Tilo Wendler

A conference managed by ACI, UK

Proceedings of the

19th European Conference on e-Learning

ECEL 2020

a Virtual Conference

Supported by

University of Applied Sciences HTW Berlin

Germany

28-30 October 2020

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

ACIL 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 ACIL 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/ECEL20 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: Prof. Dr. Tilo Wendler
E-Book ISSN: 2048-8645
Book version ISBN: Prof. Dr. Tilo Wendler
Book Version ISSN: 2048-8637

Published by Academic Conferences International Limited
Reading, UK
www.academic-conferences.org
info@academic-conferences.org

Contents

Blockchain Technologies for the Validation, Verification, Authentication and Storing of Students' Data

Alexander Pfeiffer[1 2 3], Stephen Bezzina[6], Thomas Wernbacher[2] and Simone Kriglstein[4 5]
[1]Comparative Media Studies/Writing, Massachusetts Institute of Technology (MIT), Cambridge, USA
[2]Center for Applied Game Studies, Donau-Universität Krems (DUK), Austria
[3]Department of Artificial Intelligence, University of Malta (UoM), Msida, Malta
[4]Austrian Institute of Technology GmbH (AIT), Vienna, Austria
[5]Faculty of Computer Science, University of Vienna, Vienna, Austria
[6]Ministry for Education and Employment, Floriana, Malta
alex_pf@mit.edu
simone.kriglstein@ait.ac.at
Thomas.wernbacher@donau-uni.ac.at
mail@stephenbezzina.com
DOI: 10.34190/EEL.20.009

Abstract: The rapid changes brought about by digital technologies in education offer rich, personalised and differentiated modes of e-learning. However, the anytime, anywhere access to teaching, learning and assessment material requires a paradigm shift in the conceptualisation and implementation of validation, verification, authentication and storing of students' data. This is especially relevant for accredited or certified programmes such as online bachelor or master degree courses, which quite often carry a substantial cost and relatively high time-consumption in terms of the recording and verification of students' learning credentials. Blockchain technologies offer an interesting and innovative approach for securing sensitive information in online educational environments. One of its main impetus is the ability, or rather the non-ability of retrospectively altering data which is stored on the blockchain. This indelible and unalterable nature of blockchain technologies allow for greater safeguarding when compared to conventional password-protected directories, from both within and outside the organisational e-learning environment. Furthermore, the open nature of public blockchains, supports decentralised data verification, hence independent of any central authority and consequently valid across different programmes, departments, institutions and countries. This also extends beyond traditional formal learning institutions, such as non-formal or informal education, but more importantly, it offers an easy and inexpensive way for businesses and job providers to safely and securely verify prospective employees' credentials. The aim of this paper is to critically evaluate the role of blockchain technologies in e-learning, by discussing the challenges, prospects and implications of implementation of this new technology to prevent identity fraud in online (as well as traditional) learning contexts and securely and irrevocably store students' data. This includes issues relating to students' records, transcripts, identity and badges, but also the provision of infrastructure security and smart contracts in online learning environments.

Keywords: Blockchain, DLT, e-learning, validation, verification, authentication

1. Introduction

The rapid changes brought about by digital technologies in education offer rich, personalised and differentiated modes of e-learning. However, the anytime, anywhere access to teaching, learning and assessment material requires a paradigm shift in the conceptualisation and implementation of validation, verification, authentication and storing of students' data. This is especially relevant for accredited or certified programmes such as online bachelor or master degree courses, which quite often carry a substantial cost and relatively high time-consumption in terms of the recording and verification of students' learning credentials.

Blockchain technologies offer an interesting and innovative approach for securing sensitive information in online educational environments. One of its main impetus is the ability, or rather the non-ability of retrospectively altering data which is stored on the blockchain. This indelible and unalterable nature of blockchain technologies allow for greater safeguarding when compared to conventional password-protected directories, from both within and outside the organisational e-learning environment. Furthermore, the open nature of public blockchains, supports decentralised data verification, hence independent of any central authority and consequently valid across different programmes, departments, institutions and countries. This also extends beyond traditional formal learning institutions, such as non-formal or informal education, but more importantly, it offers an easy and inexpensive way for businesses and job providers to safely and securely verify prospective employees' credentials. The current COVID-19 situation has shown that during times of massive travel restrictions, problems with mailings and even complete lock-down, we need to have digital capabilities where secure, non-manipulable storage of data and digital identities are combined. Even during this difficult period, school grades, certificates, employment certificates and similar documents must be issued on the one hand and checked for their validity on the other.

Non manipulative storage can be provided by Blockchain Systems. Blockchain, as we know it today, is based on the white paper "Bitcoin: A Peer-to-Peer Electronic Cash System", by the anonymous author Satoshi Nakamoto. Blockchain technologies belong to the Distributed Ledger Systems, or DLTs in short. This means that information of the same type is stored on different computers. The ledger is therefore divided into different locations, operated by different persons or companies, none of which have to know or personally agree with each other when using a public Blockchain. The special thing about Blockchains is that, according to a set of rules that varies slightly depending on the Blockchain system, transactions (in the sense of data records, for example, after a certain period of time or when a certain size of the total data volume has been reached) are combined in a block and stored in encrypted form (as a block). This process is intended to ensure that the exact same information is actually stored on the distributed systems and that there is no file or text information among them that may have the same file name and size as all the others, but does not contain the correct information. The storage process of a Blockchain is therefore based on the fact that new data blocks are continuously generated. Each of these new entries (blocks) increases the size of the Blockchain.

This results in the so-called "block height". The block height is the counting mechanism of a Blockchain. It counts up, starting with block #1, the "Genesis block" without any basic limitation. Each block is encrypted and has a unique hash value. A hash value results from the data stored in a block plus additional information such as the time, or for example random numbers that are added by the respective Blockchain according to a certain algorithm. This has the goal of ensuring the uniqueness of the hash value. Each block now starts with the hash value of the previous block and passes on its own hash value to the next block. A good metaphor would be that the blocks are stuck together with a labelled super glue. On the one hand, the connection can be seen in the chronological order to the previous and next block and on the other hand, in terms of the hash value per block. It is therefore verifiable that all blocks of the same block height verified as correct are absolutely identical on all "nodes" that store a copy of the blocks. Nodes is the name for computer systems that store a copy of the Blockchain. But why is it a decentralized system? It is a decentralized system, because the blocks which, as already mentioned, must all have the same hash value, are stored on many different computers (nodes). The way nodes agree on the correctness of the information is determined by the so-called "consensus algorithm". There are different approaches to this, which were consciously chosen depending on the purpose of the Blockchain being used. The best known are the "Proof of Work, PoW" and the "Proof of Stake, PoS" algorithm. PoW is about being the first computer to find a random number, PoS is about the percentage of network tokens you hold and a random factor that determines whether you are the first to validate a new block. This process is called "Mining" (with PoW), or "Forging" (with PoS). A node can now simply always save the valid copy of the Blockchain, or one can decide to additionally secure the Blockchain and perform further validation processes. As a reward, the "miners" or "forwarders" receive, for example, shares of the transaction fees paid. This is because every transaction made on a public Blockchain has to be paid by the sender or by a sponsor (in technical jargon sponsoring is called "bundlng"). (Schmidt 2019)

Blockchain systems can basically be operated in three different ways:

- Private Blockchain: is basically a closed system and is operated exclusively within organisations, companies or government structures. No information is passed on to the outside world unless there is evidence that a transaction has taken place.
- Blockchain operated by a consortium: serves connected parties who have a common goal. Consortium partners may join the Blockchain on the basis of joint agreements.
- Public Blockchain: has no restrictions on joining and/or leaving the Blockchain. All information is public, although it is possible to store some information in encrypted form.

Private and consortium Blockchains can also store information on a public Blockchain, for example the hash value of all transactions within 24 hours. This keeps the data content itself private but ensures that no data manipulation takes place retroactively. Not block by block, but still, as in the example above, for all data older than 24 hours.

For the purpose of secure storage and verification, the aspect of digital identities now needs to be considered. Such Digital identities can come from various sources; these can be assigned by an employer, through a service provided by a government entity (For example signatures that comply with the EIDAS regulation) an external company specializing in the creation of such signatures, the self-sovereign identity (SSI) movement (Sovrin Foundation) or generated through an interface like Facebook Connect. All these different sources offer a range of varying levels of trust, both within the institution where the signature is principally used, but especially when interacting with third parties. Ultimately, this level of trust or its valuation is a determining factor in how far the authorization of the respective digital/electronic signature goes.

The first state-supported pilot project for a digital identity on blockchain in the EU was launched in Zug, Switzerland, in September 2017 (Blockchain-Identität für alle Einwohner 2017). It is based on the Ethereum blockchain. In June 2018 these blockchain identities were officially used for voting (Eixelsberger et al. 2019, 514). Another application of digital identity is described by Giannopoulou (2020), whereas "data cooperatives" approaches using "data as a common value", strive to create tools for collective data regulation. However, community standards for data management in such projects remain opaque. If closed ecosystems of data emerge as a result, abuse and exploitation within them are technically viable. A non-authoritarian way to manage digital identities is to provide as many opportunities for integration as possible.

In this paper we critically evaluate the role of blockchain technologies in e-learning from different disciplines by discussing the challenges, prospects and implications of implementation of this new technology to prevent identity fraud in online (as well as traditional) learning contexts and securely and irrevocably store students' data. This includes issues relating to students' records, transcripts, identity and badges, but also the provision of (technical) infrastructure security and smart contracts in online learning environments.

2. Related work

Grech and Camillieri (2017) have been at the forefront of research into blockchain technologies for the education sector. They are the authors of the report "JR science for policy reports: Blockchain in Education", which was published in 2017. According to them, the transfer of data sets into the Blockchain and the rapid verification of their validity opens up new avenues for action. According to Grech and Camilleri (2017), Blockchain technologies have the following advantages:

- self-determination, which means that users can identify themselves while retaining control over the storage and management of their personal data;
- trust, i.e. for a technical infrastructure that gives people enough confidence in how it works to be able to carry out transactions such as payments or the issuing of certificates;
- transparency & origin, i.e. for users to carry out transactions in the knowledge that each party has the ability to make that transaction;
- immutability, i.e. that the records can be written and permanently stored without the possibility of modification;
- impartiality, i.e. the elimination of the need for a central controller to manage transactions or keep records;
- collaboration, i.e. the ability of the parties to negotiate directly with each other without the need to mediate third parties.

Grech and Camilleri (2017) describe that Blockchain in the educational sector is still in its beginning, but they see the following use cases in the near future:

- creation of digital certificates/certificates or creation of digital proof of authenticity of printed certificates;
- storage of proofs of performance after examinations including meta data;
- recognition of examination results between and within educational institutions;
- use of a personal "lifelong learning" directory (virtual CV);
- verification of the authenticity of the certificates by third parties (e.g. personnel managers authorised by applicants);
- management of intellectual property, e.g. in the context of project implementation;
- processing of payments.

The authors further describe various basic assumptions that need to be made in order for Blockchain to establish its place in the educational sector

- open implementations of the technology;
- use the open source software;
- use open standards for data;
- implement self-managed data management solution;
- further developments must be driven forward jointly by market participants and regulators / authorities.

Grech and Camilleri (2017) also note that it is often easier to create centralized solutions with a commercial background, than truly decentralized approaches.

In an earlier conference paper, Pfeiffer et. al (2019) considered where blockchain can be used in education. In an online survey, people from the IT industry and the education sector were asked about this topic.

All Interviewees together (multiple responses possible)	Weighted Average
Handle payment transactions, for example for course fees	4,25
Taking exams "off-school/university/education center", assuming a suitable ID-checking solution is in place	4,11
Storing the successful completion of a course or class, without any specific grades	4,09
Storing grades at the end of the term	4,03
Handling of voting (e.g. vote for school representatives)	4,01
Scholarship processing and funding management	3,79
Storing competence profiles at the end of the term	3,73
Storing each test completed that has been completed during a term	3,62
Adapting digital serious games for use as assessment tools	3,61
Storing each step/chapter of an exam through e-learning tools while being examined	3,44
Class book and validated communication with parents/relatives	3,27
Storing a behavioural grade at the end of the term	3,2
All interviewees n=144 / skipped 6 | Scale 7 = highly agree, 1 = do not agree	

A brief extract from this survey shows that with a score above 4, two classic applications of blockchain are mentioned: Payment (e.g. of tuition fees) and voting (e.g. of the school or university student representative). Also mentioned, with a score just over 4, are the storage of diplomas, year-end transcripts and exams taken from outside school or university (if there is a target-oriented solution for digital identity). Only minimally above the average, are areas such as the behavioural grade, the recording of every (even the smallest) test achievement or the class register.

Another part of this survey asked which steps are necessary for Blockchain technologies to gain a foothold in the educational system:

All Interviewees together (multiple responses possible)	Weighted Average
Basic information/education about blockchain-technologies for all people involved in the educational sector	4,17
Sophisticated privacy-settings	4,17
Clear and transparent rules about who is responsible for payment of fees	4,17
In-depth education about blockchain-technologies for IT-professionals and administrative-officers in the educational-sector	4,15
The ability to get a copy of my own data that can be stored on my own node, regardless of which blockchain system was originally used.	3,82
The possibility to process information from various blockchain-systems	3,78
Everything has to be set up with open-source technologies	3,74
The ability to operate a full node and store an encrypted copy of the blockchain used to store credentials	3,48

All Interviewees together (multiple responses possible)	Weighted Average
Having a close look if and which patents are involved within the used technology	3,39
Involvement of Government, strict worldwide regulation	3,01
Involvement of Government, strict local regulation	2,86
Involving corporations in the process of setting up Blockchain-technologies in the educational sector	2,86
All interviewees n=144 / skipped 6 | 7 = highly agree, 1 = I do not agree with this step	

With 4.17 clearly above the average, a basic training for all persons from the education sector, a well-defined solution as to how and who pays the transaction fees (should a public blockchain be used) and a modern solution in the area of privacy settings were ranked. Further relevant points are an in-depth training for the IT staff in the education sector, a solution that includes different blockchain systems, the open-source idea and the possibility to have your own data, or even to operate your own node. The interviewees are undecided in the area of regulation and whether large companies should push the developments. Here the score is even below average (2.86).

3. Aim of this research and methodology

The aim of this paper is to critically evaluate the role of blockchain technologies in e-learning and assessment, by discussing the challenges, prospects and implications of implementation of this new technology to prevent identity fraud in online (as well as traditional) learning contexts and securely and irrevocably store students' data. This includes issues relating to students' records, transcripts, identity, and badges, but also the provision of infrastructure security and smart contracts in online learning environments. Desk research, complemented by a guided group discussion of the author team, was utilised to gain an understanding of existing literature and shed light on potential ways forward. The results of the group discussion are presented in the next section.

4. Findings

In the near future, there might be a number of different educational credit systems similar to blockcerts, a solution originally built at MIT using a 1-way hash function to store learning credentials on the Bitcoin Blockchain. These educational credit systems are likely to be built upon a variety of different Blockchain systems, and different institutions (such as universities, colleges and schools) will also use different credit systems. A possible solution to this problem would be an independent mediator that collects and validates the credentials issued on the various systems. Such a mediating system could serve as a "collection point", compiling and validating the results of the various credential systems and connecting them to the users digital ID (e.g. the "Handy-Signature" (a citizenship card on the mobile phone issued by the Austrian government, or (within the EU) other digital identity procedures within the EIDAS (Electronic Identification, Authentication and trust Services) regulation), making it possible for users to access their own data and share it as proof of achievement (e.g. as a link in their CV).

Another reason why such an independent mediating system might be useful or even necessary, is the possible dependency on the provider of a Blockchain-based application. This is mainly due to these credential systems not being based on open-source, public, permission-less Blockchains, but instead are developed to operate on centralized, controlled Blockchains, owned by private companies, who intend to sell their systems to governments and universities. For instance, Sony corporation has recently developed such a system, based on a patent the company holds, and is currently marketing it to schools and universities. While this company might successfully sell its system to an educational institution and might even provide an excellent service in handling this institution's processes regarding test results, credentials, admissions, etc., it is still possible that, for whatever reasons, the company decides to shut down its centralized permissioned Blockchain at a later point. Without an independent mediating system, the data would almost certainly be lost, defeating the purpose of using a Blockchain-system altogether. If, on the other hand, the data was compiled at a universal "collection point", together with the data from all the other credential systems, a verified copy of the results would still exist on a public permission-less Blockchain and could be stored on this (de-centralized) Blockchain, potentially forever. Such a system would provide the security of a decentralized Blockchain even for centralized-Blockchain applications, enabling anyone to run a full node at low costs that acts as a public ledger, and ensuring that the Blockchain and its entries will exist unless everyone in the world including yourself is shutting down the node.

Other potentially challenging issues (both technologically, as well as financially) include the number of transactions that can be handled within a certain period, the respective transaction costs and who is responsible in payment terms (because on a public Blockchain transactions usually cost a certain amount of money, commonly paid in the native token of the specific Blockchain). As a university using blockcerts, one might only have to issue the learning credentials twice a year to each student. In this case, the number of transactions is still easily manageable, and the transaction fees (amounting to two times the number of students, multiplied by the fees payable to the network), will be in the affordable range. However, using Blockchain-technologies, even for basic E-Learning and E-Assessment applications, leads to a much higher number of transactions, as not only the final grades would be entered in the Blockchain, but the results from each single test, and maybe even the answers to specific questions.

The greatest number of transactions, however, occur when game-based assessments (and especially Integrated Game-based Learning/Assessment (GBL/A) solutions - This means that the Serious Game continuously measures the exam performance during the game process.) make use of Blockchain-systems. In addition to milestones reached and badges awarded, every individual step learners take inside the game world, might be stored on the blockchain. The aggregation of this data leads to a test result which is subsequently reflected in a final grade. This enormous amount of transactions is necessary to reach the goal of immutability and consistency and the possibility of learning credentials that do not only show the end results, but also record all steps in between, leading to the final grade/s. Due to this considerable number of transactions, game-based learning assessment calls for especially robust Blockchain systems, and as these transactions will need to be nearly instant as well as cost effective, strategies that enable more efficient transaction management (using, for instance, mechanics like bundling, pruning, proof-of-existence-secure timestamps using merkle-trees) will be in high demand. In all aforementioned cases, it should also be possible to develop Blockchain-enabled learning and assessment environments, without the player/learner having to hold tokens of the Blockchain-system used by him/herself. Moreover, the system has to offer an interface which can easily be used by third parties (e.g. educational software providers), while still being immutable at the same time. Thus, future research projects in this regard are of utmost importance.

A Blockchain-based system must therefore be extremely robust in order to handle the enormous amount of transactions that occur using game-based assessments (and especially GBL/A) approach. Any system that is strong enough to handle this volume of transactions will easily handle more simple demands like E-Learning assessments or storing the final grading results at the end of each semester. Hence, by focusing on Blockchain solutions for GBL/A as a long-term goal, one will also ensure that its findings will be applicable for less demanding applications, making them highly relevant not only for the educational sector as a whole, but also for Blockchain-developers who are interested in stable and sustainable Blockchain-applications.

Another important issue that differs, but cannot be dealt separately from technological problems, is the human factor, or more specifically, the role humans play in the process of creating, storing and managing data on the Blockchain. While safekeeping data on a Blockchain is primarily a technical process, the data itself (at least some of the educational data, like grades) is often produced by human agents. Consequently, the following issues must at least be kept in mind when developing future Blockchain-in-education scenarios:

(i) Humans as a source of error

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 caused by 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 favourite student's attendance times, 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 could easily be ruled out.

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: when a professor takes an exam, tells his assistant to note the grade, which is then dropped off at a secretary's desk, whom finally emails the grade to the Blockcert-department for secure entry in the Blockchain. This process offers many opportunities for human error, ranging from unfair grading by the professor, to the assistant mixing up U.S. and European grading scales, to the secretary mistyping when copying the grade, to the Blockcert-clerk assigning the grade to the wrong student. This problem can be reduced when a whole (basic, gamified combined or even integrated game-based) E-learning and Assessment system is based on the Blockchain, as this allows the immediate storage of test results, and to ensure that grades are calculated based on a grading fixed key and in real time. While the initial creation of the test (including how answers and actions are evaluated, and determination of the grading key) is still subject to human error, it is the system that provides transparent testing conditions for every student, saves the (intermediate and final) results immediately and securely, and safeguards this data from retroactive manipulation.

(ii) Dealing with faulty entries

While Blockchain-based systems can ensure the immutability of data, this also creates problems when it turns out that this data has been created based on faulty premises. The more obvious reason for faulty data entries has already been described on the example of systems which only use Blockchain technologies to store final grades, as there is a great number of reasons that can lead to a wrong grade being entered in the Blockchain. And even when a sophisticated E-learning and Assessment system ensures that grades are always correctly calculated in accordance with the grading key, mistakes in determining the grading key or in setting the correct and incorrect answers in a test cannot be ruled out.

If it turns out that the wrong grades have been saved, or if the learner has improved his grade on a new attempt of the test (or it has stayed the same, or even worse, but definitely with a new timestamp), they still cannot be changed. Instead, additional entries must be made that contain not only the correct grade, but also the information that the previous grade has been entered incorrectly into the system. This is because corrections cannot be made as edits, but only as additions to existing entries. In this sense, Blockchain-based systems might require a radical re-thinking of educational credentials, as these systems no longer highlight the learner's successes, but instead serve as a comprehensive learning biography, in which successes, stagnation and failures are equally reflected.

5. Conclusion

The arguments put forward by Grech and Camilleri (2017), are still not only valid for todays' contexts, by remain highly relevant and deserve further examination. General understanding of blockchain technologies can still be considered very low. Open source solutions are essential for a broad and real use of blockchain technology, but these do not seem to be desirable by governments and large technology companies. Privacy settings, digital identities such as SSI (Self Sovereign Identity), qualified signatures and the processing and ownership of personal data have to be further investigated and thoroughly considered.

6. Future research

The team of authors, consisting of experts from various universities and governmental units in Europe and the USA, is currently investigating the issues and problems presented in this research paper. Special attention is and will be devoted to the points listed in the conclusion. However, one of the biggest hurdles is still the big dispute between the fans / developers of the different blockchain systems.

References

Eixelsberger, W., Manfred W. und Walter, H.. (2019). Blockchain in der Verwaltung. Handbuch E-Government. Springer Fachmedien Wiesbaden, pp. 506-518. https://doi.org/10.1007/978-3-658-21402-9_43

Giannopoulou, A. (2020). Algorithmic Systems: The Consent Is in the Detail? *Internet Policy Review* 9, no. 1 (March 23). https://policyreview.info/articles/analysis/algorithmic-systems-consent-detail.

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

Nakamoto, S. (2008). Bitcoin: a peer-to-peer electronic cash system. Available at: https://bitcoin.org/bitcoin.pdf

Pfeiffer, A., Bezzina, S., Wernbacher, T. & Kriglstein, S. (2020). THE ROLE OF BLOCKCHAIN TECHNOLOGIES IN DIGITAL ASSESSMENT. 10.13140/RG.2.2.35016.75522. (accepted for EDULEARN 2020, preprint from Researchgate.net)

Schmidt, N. (2019) Kryptowährungen und Blockchains, Technologie, Praxis, Recht, Steuern, Linde Verlag, Wien

Tobin, A., and Reed, D. (2016). The Inevitable Rise of Self-Sovereign Identity. The Sovrin Foundation