Tennessee TECH

OAK RIDGE National Laboratory

Proceedings of the 16th International Conference on Cyber Warfare and Security

Tennessee Tech University and Oak Ridge National Laboratory
Cooksville, Tenessee, USA
25-26 February 2021

Dr. Juan Lopez Jr., Dr. Ambareen Siraj and Dr. Kalyan Perumalla

aci

A conference managed by ACI, UK

Proceedings of the

16th International Conference on Cyber Warfare and Security ICCWS 2021

A Virtual Conference Hosted By

Tennessee Tech University and the Oak Ridge National Laboratory USA

25-26 February 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
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 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/ICCWS21 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: 978-1-912764-88-4
E-Book ISSN: 2048-9889
Book version ISBN: 978-1-912764-87-7
Book Version ISSN: 2048-9870
Published by Academic Conferences International Limited
Reading, UK
+44-118 324 6938
www.academic-conferences.org
info@academic-conferences.org

Contents

Preface

These proceedings represent the work of contributors to the 16th International Conference on Cyber Warfare and Security (ICCWS 2021), hosted by joint collaboration of Tennessee Tech Cybersecurity Education, Research and Outreach Center (CEROC), Computer Science department and the Oak Ridge National Laboratory, Tennessee on 25-26 February 2021. The Conference Co-Chairs are Dr. Juan Lopez Jr, Oak Ridge National Laboratory, Tennessee, and Dr. Ambareen Siraj, Tennessee Tech's Cybersecurity Education, Research and Outreach Center (CEROC), and the Program Chair is Dr. Kalyan Perumalla, from Oak Ridge National Laboratory, Tennessee.

ICCWS is a well-established event on the academic research calendar and now in its 16th year, the key aim remains the opportunity for participants to share ideas and meet the people who hold them. The conference was due to be held at Tennessee Tech University, Cookeville Tennessee, but due to the global Covid-19 pandemic it was moved online to be held as a virtual event. The scope of papers will ensure an interesting two days. The subjects covered illustrate the wide range of topics that fall into this important and ever-growing area of research.

The opening keynote presentation is given by Dr. Deborah Frincke, Associate Laboratory Director for National Security Sciences at Oak Ridge National Laboratory, USA, on the topic of *"What's Science Got to Do With it?".* The second day of the conference will open with an address by Ms. Diane M. Janosek, Deputy Commandant for the National Cryptologic School, NSA on the topic of *Cyber Partnerships for the Future.*

With an initial submission of 140 abstracts, after the double blind, peer review process there are 47 Academic research papers, 2 PhD research papers, 6 Masters Research papers, 2 Non-Academic papers and 4 work-in-progress papers published in these Conference Proceedings. These papers represent research from Australia, Austria, Brazil, Croatia, Estonia, Finland, France, Germany, Ireland, Morocco, Romania, Russia, South Africa, UK, and the USA.

We hope you enjoy the conference.

Dr. Juan Lopez Jr., Dr Kalyan Perumalla and Dr. Ambareen Siraj
Oak Ridge National Laboratory and Tennesse Tech University,
Tennessee
USA
February 2021

ICCWS Conference Committee

Dr. Kareem Kamal A.Ghany, Beni-Suef University,, Egypt; Prof Azween Abdullah, Taylors University, Malaysia; Dr William ("Joe") Adams, Univ of Michigan/Merit Network, USA; Assc Ali Al Mazari, ALFAISAL University PS-CoB, Saudi Arabia; Prof Hamid Alasadi, Iraq University college, Iraq; Dr Elie Alhajjar, USMA, USA; Prof. Todd Andel, University of South Alabama , USA; Prof. Antonios Andreatos, Hellenic Air Force Academy, Greece; Dr. Leigh Armistead, Edith Cowan University, Australia; Leigh Armistead, Oak Ridge National Laboratory, USA; Researcher Jawad Awan, Institute of Information & Communication Technology, Pakistan; Mrs Stacey Baror, University of Pretoria, South Africa; Prof. Richard Baskerville, Georgia State University, USA; Dr Zakariya Belkhamza, Ahmed Bin Mohammed Military College, Qatar; Dr. Noam Ben-Asher, IBM/US Army Research Lab, USA; Prof Vijay Bhuse, Grand Valley State University, USA; Prof. Alexander Bligh, Ariel University Center, Ariel, Israel; Dr. Svet Braynov, University of Illinois, Springfield, USA; Dr. Raymond Buettner, Naval Postgraduate School, USA; Dr. Acma Bulent, Anadolu University, Eskisehir, Turkey; Ivan Burke, CSIR, Pretoria, South Africa; Dr Mustafa Canan, Naval Postgraduate School, USA; Dr. Jim Chen, U.S. National Defense University, USA; Mr Ben-Douglas Christie, , UK; Prof. Sam Chung, University of Washington, Tacoma, USA; Dr. Nathan Clarke, University of Plymouth, UK; Dr. Ronen Cohen, Ariel University Centre, Israel; Mr Edwin Covert, WarnerMedia, USA; Dr Paul Crocker, University of Beira Interior, Portugal; Dr. Michael Dahan, Sapir College, Israel; Geoffrey Darnton, Requirements Analytics, UK; Dr. Dipankar Dasgupta, University of Memphis, USA; Evan Dembskey, UNISA, South Africa; Dorothy Denning, Naval Post Graduate School, USA; Dr. Glenn Dietrich, University of Texas, Antonio, USA; Prokopios Drogkaris, University of the Aegean, Greece; Prof. Mariki Eloff, University of South Africa, South Africa; Prof. Eric Filiol, ENSIBS, Vannes, France & CNAM, Paris, France; Larry Fleurantin, Fleurantin, Francois & Antonin, P.A., North Miami Beach, USA; Dr Noluxolo Gcaza, Tshwane University of Technology, South Africa; Dr. Ahmad Ghafarian, University of North Georgia, USA; Dr Scott Graham, Air Force Institute of Technology, USA; Prof. Dr. Tim Grant, Retired But Active Researcher, The Netherlands; Dr John Gray, Nova Southeastern University, USA; Virginia Greiman, Boston University, USA; Dr. Michael Grimaila, Air Force Institute of Technology, USA; Daniel Grosu, Wayne State University, Detroit, USA, USA; Dr. Per Gustavsson, Combitech / Swedish Defence University / George Mason Univeristy, Sweden; Dr Ulrike Hugl, University of Innsbruck, Austria; Dr. John Hurley, National Defense University, USA; Prof. Bill Hutchinson, Edith Cowan University, Australia; Dr. Berg Hyacinthe, State University of Haiti, Haiti; Prof. Barry Irwin, Noroff, Oslo, Norway; Ramkumar Jaganathan, VLB Janakiammal College of Arts and Science (affiliated to Bharathiar University), India; Prof. Leonard Kabeya Mukeba Yakasham, ESURS/ISTA-KIN & ASEAD, DR Congo; Dr Ezhil Kalaimannan, University of West Florida, USA; Dr Bilge Karabacak, Freelance, USA; Dr Saltuk Karahan, Old Dominion University, USA; ; Prof Jesuk Ko, Universidad Mayor de San Andres, Bolivia; Dr Anne Kohnke, Lawrence Technological University, USA; Dr Ahmet Koltuksuz, Yasar University, Turkey; Dr Maximiliano Korstanje, University of Palermo, Buenos Aires, Argentina, Argentina; Michael Kraft, CSC, USA; Prashant Krishnamurthy, University of Pittsburgh, USA; Prof. Hennie Kruger, North-West University, South Africa; Mr. Peter Kunz, DoctorBox, Germany; Rauno Kuusisto, Finnish Defence Force, Finland; Dr Gregory Laidlaw, University of Detroit Mercy, USA; Dr Arash Lashkari, UNB, Canada; Dr Sylvain (Sly) Leblanc, Royal Military College of Canada, Canada; Louise Leenen, CSIR, Pretoria, South Africa; Prof Martti Lehto, University of Jyväskylä, Finland; Dr Antoine Lemay, École Polytechnique de Montréal, Canada; Dr. Andrew Liaropoulos, University of Piraeus, Greece; Mr Trupil Limbasiya, NIIT University, Neemrana, Rajasthan,India; Juan Lopez, Oak Ridge National Laboratory,USA; Volodymyr Lysenko, University of Washington, USA; Dr. Bill Mahoney, University of Nebraska, Omaha, USA; Dr Naufal Mansor, Kampus Uniciti Alam,, Malaysia; Dr Naufal Mansor, Kampus Uniciti Alam,, Malaysia; ASSI Haribabu Maruturi, qiscet, india; Dr Paul Maxwell, Army Cyber Institute, USA; Dr. Todd McDonald, Air Force Institute of Technology, USA; Dr. Robert Mills, Air Force Institute of Technology, USA; Dr Pardis Moslemzadeh tehrani, University of Malaya, malaysia; Dr. Barry Mullins, Air Force Institute of Technology, USA; Prof Antonio Muñoz, University of Málaga, Spain; Dr. Lilian Nassif, Public Ministry of Minas Gerais, Brazil; Dr Asoke Nath, St. Xavier's College(Autonomous), India; Daniel Ng, C-PISA/HTCIA, China; Dr Emmanuel OGU, Babcock University, Ilishan-Remo, Ogun State., Nigeria; Dr. Funminiyi Olajide, Nottingham Trent University, UK; Mr Arif Mohamed Ismail Oliullah, Jefferies International Lts, UK; Prof. Abdelnaser Omran, School of Economics, Finance and Banking, Universiti Utara Malaysia, Malaysia; Prof. Dr. Frank Ortmeier, Otto-von-Guericke Universität, Magdeburg, Germany; Rain Ottis , Tallinn University of Technology, Estonia; Prof. Evgeny Pashentsev, Diplomatic Academy of the Ministry of Foreign Affairs of the Russian Federation, Russia; Prof. Graham Payne, Old Dominion University, Virginia, USA; Kalyan Perumalla, Oak Ridge National Laboratory, USA; Dr. Gilbert Peterson, , USA; Pete Peterson, Ministry of Foreign Affairs of the Russian Federation, USA; Rodney Peterson, NIST, US Gov , USA; Andy Pettigrew, George Washington University, USA; Dr. Jackie Phahlamohlaka, Council for Scientific and Industrial Research, Petoria, South Africa; Ms Heloise Pieterse, CSIR, South Africa; Dr Bernardi Pranggono, Sheffield Hallam University, UK; Prof Carlos Rabadão, Politechnic of Leiria, Portugal; Dr Trishana Ramluckan, University of KwaZulu-Nata, South Africa; Prof. Aunshul Rege, Temple University, USA; Dr. Ken Revett, British University, Egypt; Lieutenant Colonel Ernest Robinson, U.S. Marine Corps / Air War College, USA; Dr. Neil Rowe, US Naval Postgraduate School, Monterey, USA; Prof. Lili Saghafi, Canadian International College, Montreal, Canada; Dr Char Sample, US Army Research Laboratory, USA; Ramanamurthy Saripalli, Pragati Engineering College, India; Dr. Mark Scanlon, University College Dublin, Ireland; Corey Schou, Idaho State University, USA; Dr. Yilun Shang, Singapore University of Technology and Design, Singapore; Dr. Dan Shoemaker, Centre for Assurance Studies, USA; Prof. Ma Shuangge, Yale University, USA; Mr. Paul Simon, Air Force Institute of Technology, USA; Ambareen Siraj, ,; Dr. Elena Sitnikova, University of South Australia, Australia; Prof. Aelita Skarzauskiene, Mykolas Romeris University, Lithuania; Ass. Prof. Dr. Risby Sohaimi, National Defence University of Malaysia, Malaysia; Dr. Joseph Spring, University of Hertfordshire, UK; Dr. William Spring, University of Hertfordshire, UK; Dr. Kevin Streff, Dakota State University, USA; Dennis Strouble, Air Force Institute of Technology, USA; Dr. Arwin Sumari, State Polytechnic of Malang, Java, Indonesia; Dr Hamed Taherdoost, Research Club, Research and Development Department of Hamta Group, Hamta

Business Solution, Malaysia; Mr. Unal Tatar, University at Albany - SUNY, USA; Pardis Moslemzadeh Tehrani, University of Malaya,; Peter Thermos, Columbia Univeristy/Palindrome Technologies, USA; Dr. Bhavani Thuraisingham, University of Texas at Dallas, USA; Dr. Socaciu Tiberiu, University of Suceava, Romania; Mr. Patrick Tobin, University College Dublin, Ireland; Dr Antonio Jorge Tomeu-Hardasmal, University of Cadiz, Spain; Dr Hong-Ngoc Tran, University College Dublin, Ireland; Dr Eric Trias, Air Force Institute of Technology, USA; Dr. Chia-Wen Tsai, Ming Chuan University, Taiwan; Brett van Niekerk, University of KwaZulu-Natal, South Africa; Dr Namosha Veerasamy, Council for Scientific and Industrial Research, South Africa; Stylianos Vidalis, School of Computer Science, University of Hertfordshire, UK; Prof. Kumar Vijaya, High Court of Andhra Pradesh, India; Dr. Natarajan Vijayarangan, Tata Consultancy Services Ltd, India; Dr Khan Ferdous Wahid, Airbus Group, Germany; Prof. Murdoch Watney, University of Johannesburg, South Africa; Richard Wilson, Towson University, USA; Hongyi Wu, Old Dominion University, Virginia, USA; Enes Yurtoglu, Turkish Air War College, Turkey; Dr. Zehai Zhou, University of Houston-Downtown, USA

Biographies

Conference and Programme Chairs

Dr. Juan Lopez Jr., USMC (ret) is a cyber-physical R&D program manager at Oak Ridge National Laboratory located in Oak Ridge, TN. He leads research in Critical Infrastructure Protection, Supervisory Control and Data Acquisition (SCADA) systems, Nuclear Power Cybersecurity, and Electromagnetic Interference (EMI) modeling. He served as the technical lead in SCADA/ICS research at the Air Force Cyberspace Technical Center of Excellence located at the Air Force Institute of Technology on Wright-Patterson AFB, OH. Dr. Lopez earned a Ph.D. in Computer Science at the Air Force Institute of Technology, Bachelor of Science from the University of Maryland, Master of Science from Capitol College, and Master of Science from the Air Force Institute of Technology under the NSA's Information Assurance Scholarship Program. Dr. Lopez is an IEEE Senior Member, Co-Chair for the Industrial Society of Automation's Work Group 4, Task Group 7 (Security of ICS Sensors), Certified Information Systems Security Professional (CISSP), Certified SCADA Security Architect (CSSA), Certified Scrum Master, Lean Six Sigma Green Belt, and has an Extra Class amateur radio license from the Federal Communication Commission (FCC).

Dr. Ambareen Siraj is a professor of Computer Science and the founding director of Tennessee Tech's Cybersecurity Education, Research and Outreach Center (CEROC). She has served as the leader on several NSF and NSA education and workforce development grants. Siraj is also the founder of the Women in CyberSecurity (WiCyS) organization, an initiative to recruit, retain and advance women in cybersecurity. Her efforts to educate students and enhance the cybersecurity field of study goes beyond classes, research, outreach projects, workshops and conferences. Dr. Siraj's research focus is on security in cyber-physical systems, Internet of Things, situation assessment in network security, security education and workforce development. She has authored or co-authored more than 50 publications. She is a frequent speaker in various cybersecurity conferences on topics ranging from education, curriculum, workforce development, outreach, security issues & solutions for cyber-physical systems to diversity and inclusion in cybersecurity. Dr. Siraj is recipient of the Colloquium for Information Systems Security Education Exceptional Leadership in Education Award in 2018.

Dr. Kalyan Perumalla is a Manager and Distinguished Scientist at the Oak Ridge National Laboratory. He founded and currently leads the Discrete Computing Systems Group in the Computer Science and Mathematics Division at ORNL. He also serves as an Adjunct Professor at the Georgia Institute of Technology and as a Joint Full Professor in Industrial Engineering at the University of Tennessee. He was a Fellow of the Institute of Advanced Study at Durham University, UK, and a member of the National Academy of Sciences' Technical Advisory Boards for the U.S. Army Research Laboratory. Dr. Perumalla is among the first recipients of the U.S. Department of Energy Early Career Award in high-performance computing. Over the past 20 years, he has served as a principal investigator (PI) or co-PI on several research projects sponsored by government agencies including the Department of Energy, Department of Homeland Security, Air Force, DARPA, Army Research Laboratory, National Science Foundation, and industry.

Keynote Speakers

Dr Deborah Frincke is the Associate Laboratory Director for National Security Sciences at Oak Ridge National Laboratory who guides the research and development of science-based solutions to complex threats. She recently was appointed as the U.S. representative to the NATO Emerging and Disruptive Technologies Advisory Board and was named a Fellow of ACM, the world's largest association of computing professionals. Deborah joined ORNL from the National Security Agency (NSA), where she served in three roles between 2011 and 2020. Her most recent role (until early 2020) was as the Director of the Research Directorate at NSA, where she led the largest in-house research organization in the U.S. Intelligence Community. She was also a founding member of the NSA Board of Directors and the first NSA Innovation Champion. Prior to joining NSA, she had a threefold career encompassing academia, reaching the rank of full professor at University of Idaho; serving as Chief Scientist for Cybersecurity at Pacific Northwest National Laboratory; and launching a successful cybersecurity startup company, TriGeo Network Systems. She has published approximately 200 articles and technical reports.

Diane M. Janosek is an award-winning cybersecurity leader and sought-after speaker. As an innovator, she has been a member of the Defense Intelligence Senior Executive Service (SES) since 2012. She currently serves as the National Security Agency's Commandant of the National Cryptologic School, which is comprised of four colleges, to include the Colleges of Cyber and Cryptology. In her role, she manages and oversees the delivery of unique courses for the U.S. intelligence workforce, both civilian and military, in the areas of cyber, network security, cyber resilience, and encryption, ensuring a strong federal workforce to defend critical national security networks. Ms. Janosek's areas of expertise include academic leadership, privacy and technology, governance and data policy, export control, defense acquisition, information and cyber security. In

her current role, she is committed to the educational, leadership, professional and practical learning needs of the nation's cyber workforce in today's dynamic threat environment.

Mini Track Chairs

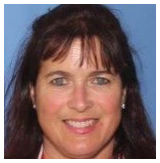
Dr. Jim Q. Chen, Ph.D. is Professor of Cyber Studies in the College of Information and Cyberspace (CIC) at the U.S. National Defense University (NDU). His expertise is in cyber warfare, cyber deterrence, cyber strategy, cybersecurity technology, artificial intelligence, and machine learning. Based on his research, he has authored and published numerous peer-reviewed papers, articles, and book chapters on these topics. Dr. Chen has also been teaching graduate courses on these topics. He is a recognized expert in cyber studies and artificial intelligence.

Dr Noluxolo Gcaza is passionate about making cybersecurity accessible to different contexts. Her research interests include cyber security governance, cybersecurity awareness and education. Currently she is a Research Group Leader at the Council for Scientific and Industrial Research (CSIR). She serves on the Advisory Board of the Center for Research in Information and CyberSecurity (CRICS) at Nelson Mandela University. Dr Gcaza also served as a Board Member in SaveTnet, a non-profit organization that focuses on fostering a culture of cyber security in a community setting through spreading cyber security awareness. She contributes in the SABS standardisation process as a committee member of the Information Security Technical Committee.

Dr Maanak Gupta is an assistant professor in computer science at Tennessee Tech University. He received his PhD from the University of Texas at San Antonio. His primary area of research includes security and privacy in cyber space. He works in machine learning and AI assisted cyber security solutions. He received the UTSA CS Outstanding Doctoral Dissertation Award in 2019. His website is: www.maanakgupta.com

Dr. Greg Laidlaw, DMIT, CISSP, C|EH, serves as the Department Chair and Lecturer in the Cybersecurity & Information Systems Department at the University of Detroit Mercy. Greg's research focuses on secure systems, secure analytics, and machine learning. Prior to transitioning into full-time academia in 2011, Greg developed an extensive range of technical and managerial experience from 25 years of IT consulting in small enterprise and local government organizations. His doctoral dissertation involved adapting agile methodologies to design and expediting a data integration project for a local Sheriff's Department.

Dr Akond Rahman is an assistant professor at Tennessee Tech University. His research interests include DevOps and Software Security. He graduated with a PhD from North Carolina State University. He won the Microsoft Open Source Challenge Award in 2016, the ACM SIGSOFT Doctoral Symposium Award at ICSE in 2018, the ACM SIGSOFT Distinguished Paper Award at ICSE in 2019, and the NC State CSC Distinguished Dissertation Award in 2020. He actively collaborates with industry practitioners from IBM, RedHat, and others. To know more about his work visit: https://akondrahman.github.io/



Dr. Char Sample is the Chief Scientist for the CyberCore division of the Idaho National Laboratory. Her research focus areas include Artificial Intelligence, Threat Intelligence, Fake News/Deception, Data Resilience, cyber-physical systems and cultural influences on cyber events and behaviors. Dr. Sample's background includes time spent in the private sector, public sector and academia. She continues to try to merge the best features from each pf these areas to guide her research.

Dr. Unal Tatar is currently an Assistant Professor of Cybersecurity at the College of Emergency Preparedness, Homeland Security, and Cybersecurity, University at Albany. He has 15+ years of cybersecurity experience of cybersecurity in government, industry and academia. He is the former coordinator of the National Computer Emergency Response Team of Turkey. Dr. Tatar's research is funded by NSF, NSA, DOD, and Society of Actuaries. Dr. Tatar holds a BSc degree in Computer Engineering, an MS degree in Cryptography and a Ph.D. in Engineering Management and Systems Engineering. His main topics of interest are cybersecurity risk management, cyber resiliency, cyber insurance, and blockchain.

Pardis Moslemzadeh Tehrani is a senior lecturer at the Faculty of Law, University of Malaya. Her research interests lie in the areas of cyberterrorism, cyberlaw, and international humanitarian law. Pardis's research has been widely published in peer-reviewed journals and she has presented papers at national and international level conferences. She is a member of the editorial review board in several journals. She is also an international scientific member of the Australian and New Zealand Society of International Law. Pardis's most recent book is Cyberterrorism: The Legal and Enforcement Issues (World Science and Imperial College Press of London, 2017).

Dr. Benjamin Yankson is an Assistant Professor of Cybersecurity at the College of Emergency Preparedness Homeland Security and Cybersecurity. He has over 15yrs experience in various technical leadership roles in Information Technology security within Healthcare and Education. He is the former Application Manager, Critical Care Information System for the province of Ontario's (CritiCall Ontario), Canada. Dr. Yankson holds a CompTIA Security+, a B.A degree in Information Technology, a master's degree in Information Technology Security (MITS), and a Ph.D. Computer Science. His current teaching and research work focuses on IoT Security, Cybersecurity Risk Management, Threat Risk Assessment (TRA), Security Auditing/Compliance, Digital Forensics, and Privacy.

Workshop Facilitator

Dr Edwin "Leigh" Armistead is the President of Peregrine Technical Solutions, a certified 8(a) small business that specializes in Cyber Security. A retired United States Naval Officer, he has significant Information Operations academic credentials having written his PhD on the conduct of Cyber Warfare by the federal government and has published three books, in an unclassified format in 2004, 2007 and 2010, all focusing on full Information Warfare. He is also the Chief Editor of the Journal of Information Warfare (JIW) https://www.jinfowar.com/; the Program Director of the International Conference of Cyber Warfare and Security and the Vice-Chair Working Group 9.10, ICT Uses in Peace and War. Shown below are the books on full spectrum cyber warfare and the JIW:

What Role can Blockchain-Based Digital Identities Play to Counteract (Cyber)Crime in Relation to Assessment Results and Credentials in the Educational Sector? A Glimpse Into the Future

Alexander Pfeiffer[1, 2, 3], Stephen Bezzina[6], Simone Kriglstein[4, 5], Thomas Wernbacher[2], Vince Vella[3] and Alexiei Dingli[3]
[1]Comparative Media Studies/Writing, Massachusetts Institute of Technology (MIT), Cambridge, USA
[2]Center for Applied Game Studies, Danube-University 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, Austria
[6]Ministry for Education and Employment, Floriana, Malta
alex_pf@mit.edu
mail@stephenbezzina.com
simone.kriglstein@ait.ac.at
Thomas.wernbacher@donau-uni.ac.at
alexiei.dingli@um.edu.mt
vvell04@um.edu.mt
DOI: 10.34190/IWS.21.015

Abstract: The forgery and fraudulent behaviour associated with examination results and academic certificates at the different stages from storing, publishing, transfer to verification, remain a major cybercrime issue within the educational sector. In this paper, the authors discuss the technological dimension underpinning such issues and propose a system consisting of digital ID verification structures, which ensure and confirm individual access via decentralized storage like Blockchain systems, in order to minimise fraudulent activities. Based on extensive desk research and a case study (using a demonstrator) which was presented and discussed with a focus group, comprising of stakeholders with a good understanding on the topic of Blockchain technologies and digital IDs, the authors discuss how the publication, storage and transfer of educational and academic achievements may potentially be transformed due to the adoption of Blockchain technologies, especially through digital ID verification. In particular, the authors identify issues pertaining to the setting up of the chain of trust, recognition of digital IDs, non-technical expertise, costs, human interventions and cybersecurity as crucial for the successful consideration and implementation of Blockchain-based digital IDs and as areas for future work in counteracting cybercrime with regard to assessment results and credentials in the educational sector.

Keywords: digital identity, blockchain, assessment, grading

1. Introduction

One field of activity in cybercrime is the forgery of examination results and academic certificates. This mainly occurs during the transnational verification of student credentials by educational institutions, quality assurance and/or qualifications recognition entities, across different countries. However, the manipulation of examination results and certificates can also take place right within the institution, where the student is currently enrolled. For instance, marks or grades on e-learning platforms can possibly be stored without the required security and encryption and thus potentially easily hackable, even by non-IT professionals. Quite often the examination results are only stored on central systems, which are on poorly protected networks. Without specific computer knowledge, the resulting marks or grades can be easily manipulated by accessing *.txt files on the e-learning system itself. Social engineering or the psychological manipulation of individuals into performing actions or divulging confidential information, as well as bribes, also play a major role, as recent examples of SAT score manipulation in the USA have shown. In this paper, the authors discuss the technological dimension, which is one main problematic area, at the core of the forgery of examination results and academic certificates. In terms of the technological aspect, a modern system consisting of digital ID verification structures which ensure and confirm individual access via decentralized storage like Blockchain systems, can prevent fraudulent activities and cybercrime. Based on expert considerations and a current case study, this paper discusses how the publication, storage and transfer of academic achievements in the educational system may change due to the use of Blockchain technologies, especially in regard to the aspect of digital identity verification.

The need to create trust, reliability and in some cases, a sense of achievement has made it necessary to artificially re-introduce certain limitations to serve as safeguards against fraudulent behaviour. Most importantly, these safeguards limit by whom and under which conditions data can be changed. Just as a person cannot simply edit the amount of money on his/her banking account, and not just anybody can make a transfer from his/her account, certain data stored in virtual learning environments cannot be changed at will. Learning achievements are to be tied to one's learning efforts, which are again tied to the individual's personal, password-protected account; and consequently, grades can only be changed either by the system, or by a teacher, whose account will again be password-protected to prevent unauthorized persons to tamper with this data.

A recent answer to these challenges might present itself in the form of Blockchain-based technologies. As originally intended decentralized systems, Blockchains should offer by design little opportunity for tampering attempts, and especially in the case of sufficiently established, public, and permission-less Blockchain systems, manipulation becomes virtually impossible. When information is stored on the Blockchain, it cannot be altered retroactively (Atzei, 2018). In addition to giving users full control over how their data is used and providing unambiguous information about the provenance of this data, such immutability makes Blockchain systems, a reasonable technology to secure critical information like personal data and finances, but also learning achievements and educational credentials. Once learning achievements and credentials are stored in a Blockchain-based system, neither teachers nor learners, and not even system administrators or the designers of the system can change entries, remove success criteria or add additional milestones. And as this system is de-centralized, no individual access can change data entries retroactively. This implies that, if it turns out that the wrong grades have been saved, these cannot be changed. Instead, additional entries must be made, which in turn contain not only the correct grade, but also the information that the previous grade has been entered incorrectly into the system, as 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 a comprehensive learning biography, in which successes and failures are equally reflected.

Another potentially challenging issue (technologically as well as financially) is the number of transactions that can be handled within a certain period, the 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 and sometimes referred to as gas-costs). And finally, a major point is the subject of identity. This includes the identity of the learner, the identity of the examiner, the identity of the institution where the exam is taken and also the identity of the person (or maybe even the AI used for an automatic verification process) that has access to test results and certificates.

2. Research question

This last point guides our research question, with which we want to address the connection between digital identities and the storage of data on Blockchain basis.

> **What Role can Blockchain-based Digital Identities Play to Counteract (Cyber)Crime in Relation to Assessment Results and Credentials in the Educational Sector?**

3. Related research

Table 1 shows in tabular form, the relevant research projects that are related to the authors' approach.

Table 1: Related research

Authors	Topic
Eixelsberger et. al. (2019)	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.
Giannopoulou (2020)	Another application of digital identity is described by Giannopoulou, 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.

Authors	Topic
Grech and Camilleri (2017)	Grech and Camillieri 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. Grech and Camillieri describe several use-cases in regards to education that existed already in 2017, like Blockcerts from MIT.
Bartolomé et. al. (2017)	The authors summarized the major challenges for Blockchain in education in four points, similar to Grech and Camilleri from a 'year 2017' perspective: *"It is not about easy and immediate implementation for social, technological, and economic reasons. It can lead to unacceptable consequences depending on the direction it is working and the intentionality with which it has been made.* *It presents challenges in areas such as privacy, transparency, functionality, and value of the certifications, as well as "official" and public institutions.* *It concerns citizens who have seen in these years as some technological changes generates other changes not always desirable."*
Schmidt (2019)	Schmidt wrote a valuable fundamental book on Blockchain technologies from different technical but also socially relevant perspectives, such as legislation.
Nakamoto (2008)	The anonymous person Satoshi Nakamoto 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.
Pfeiffer et. al (2019)	Pfeiffer et. al. considered where Blockchain can be used in education. In an online survey, people from the IT industry and the education sector were interviewed about this topic. It is evident that there is a wide range of possible applications for Blockchain, but the knowledge of the policy makers can still be considered relatively low.
König and Pfeiffer (2019)	König and Pfeiffer discuss the use of Blockchain technologies in educational games for assessment from a humanities perspective.
Agusting et. al. (2020)	Agustin et. al describe the application of Blockchain technology in e-certificates in the open journal system. The study reports that the issuance of e-certificates in an open journal system is a way to manage and verify, prevent duplicates or even falsification of e-certificates. This project is based on Blockcerts by Learning Machine (originally developed at MIT).
Merija and Kapenieks (2018)	Merija and Kapenieks compare Blockcerts with Ethereum Smart Contracts developed by Open University, UK.
Baldi et. al (2019)	Baldi et. al. describe how to impersonate a legitimate issuer of Blockcerts certificates with the aim to produce certificates that cannot be distinguished from originals by the Blockcerts validation procedure.
Pfeiffer et. al (2020)	Pfeiffer et. al. demonstrate the use of Blockchain in the educational sector using three practical examples. A serious game for assessment, an e-learning quiz and the possibility of issuing grades after an oral exam. Results from this paper have been integrated into the concept of the demonstrator described in this paper, especially regarding digital identity and Blockchain.
Kalla et. al. (2020)	Kalla et. al. identified use-cases for Blockchain during the Covid-19 crises. They describe that "*Blockchain systems enable secure cross-platform sharing of online content and encourage automatic standardization across educational establishments. Smart contracts and tokens can be used to device correct payment system based on the exact usage of content. Decentralized blockchain-based storage increases the security of student data while ensuring it remains available to the authorized users. Finally, blockchain allows fast, efficient and secure issuance and sharing of verifiable educational credentials."*
Lee et. al (2013)	The authors show that the data transmitted from an online certificate issuing server to output devices (such as a PC or printer) can be accessed by a hacker and modified into a false certificate and that the falsified document or certificates can be printed. Furthermore, the findings show that the data located in the memory of an Internet browser that conducts the issuing of certificates can be accessed and manipulated.
Thompson and Cook (2014)	Thompson and Cook take a look at the data-driven NAPLAN testing in Australia. They argue that this database defines who is "a good or a bad teacher". Therefore, the authors conclude, that manipulating the data is a regrettable, but logical, response to manifestations of teaching where only the data counts. This paper outlines the human role and motivations in regards to manipulating test results, in this case from a perspective of improving the status of a teacher.

4. Method

To achieve their research goal, the authors carried out extensive desk research and developed a case study which was presented and discussed with a focus group. The core discussion revolved around the aspects of digital identity and what does it mean to set up a chain of trust. The focus group consisted of five participants. Table 1 details the gender and respective background for each participant.

The realization of the focus group is based on the method of the problem-centered interview following Witzel (1985), whilst the evaluation of the key statements was conducted according to Mayring's (2010) approach in regard to content-analyses. This problem-centered approach is characterised by the orientation towards a socially relevant problem (in this case the forging of test results) and the organisation of the cognition or learning process (pre-interpretation). As such, the interviewer uses the previous knowledge of objective (in this case the knowledge gained through desk research) in order to understand the interviewees' explications and ask questions or demands oriented towards the problem. Parallel to the production of broad and differentiated data material, the interviewer works on the interpretation of the subjective view of the interviewees opinions and refines this in view of the research problem. In the content analysis, in addition to the formation of categories, in this case securing learning outcomes on Blockchain, the authors have reduced the results of the interviews in the form of core statements. However, these are partially underpinned by direct quotes.

Note: All participants of the focus group have a basic to good understanding on the topic of Blockchain technologies and digital IDs.

Table 2: Participants of the focus group

Expert ID	Gender	Profession / Field
E1	female	IT Professional
E2	male	Lecturer at a university in the field of ICT
E3	male	Administrative officer at a university
E4	female	Researcher in the field of education and teacher
E5	female	Student

5. Results

5.1 Presentation of the demonstrator

At the beginning of the focus group, the authors showed the participants the underlying concepts of the demonstrator using the graphical user interface of the Ardor Testnet and the relevant screenshots. The basic assumption in this case is that a teacher (associated with a university), runs a course in which a person is registered. The participant receives a certificate of attendance and the award for the most dedicated participant.

The first step is to create the Blockchain addresses. On https://testardor.jelurida.com/ the function to create several Blockchain addresses with one "Master Seed" was chosen. For this demo this has the advantage that the authors have control over all addresses used. When creating real apps one always has to decide whether the users register with their own blockchain addresses and therefore have full control over their wallet or if there is an issuer who can intervene if there are, for example, problems with the login, such as a lost password.

The authors created three accounts, with the University account as the master account:

University: ARDOR-N34E-3DB8-ASEN-HRZKK
Teacher: ARDOR-RXMR-AJBG-DYGH-E8HH5
Student: ARDOR-T6PD-S4PF-AK2C-HJUE5

To look into the transaction, a quick and easy way is to use a block explorer. For the purpose of this paper, the URL https://test.ardorportal.org/accounts/account/17926568467623445580 lists all transactions of the main account. However, the most secure way to verify transactions is always to run a personal full node. After the authors provided the three accounts with testnet tokens of the native currencies (Ignis and Ardor) to pay all transaction fees[1], the next step was to name the accounts. The authors decided to give the accounts the name

[1] The testnet of Ardor can be found using this link: https://www.ardor.world/en/faucet_ignis/ (the tokens have no value and can be used on Testnet only)

of the respective roles within the demonstrator. Additionally, a description could be added. For the purpose of this demonstrator, this was the reference to the ICCWS2021 conference. It is always advisable to add links to registers which prove that the Blockchain address belongs to the person or institution in question.

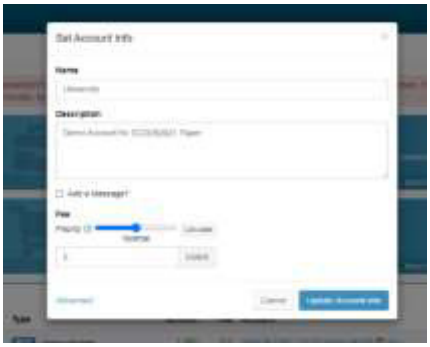


Figure 1: Naming the accounts

With regard to the 'Chain of Trust', the authors posted a message from the official account of the University Facebook account, listing the used blockchain address. It is important to note that such postings can be easily hackable, and therefore for the purpose of use-cases in the real work, such addresses would have to be stored on the official University website and/or an official database of the state University administration. In this sense, a central system helps to initiate and support the decentralized system in terms of trust.

Figure 2: Start of the chain of trust using a centralized service which posts the Blockchain main account address

The authors then sent a message to themselves through the University account. Unencrypted and stored forever on the Blockchain, this message contained the Blockchain addresses of the participating teachers and students, without revealing any further personal data.[2]

The next step was the design of the token economy. For the purpose of this demonstrator a total of 5 tokens were created. Each token has its own Asset-ID on the Blockchain and serves a specific purpose. The authors wanted to build on the findings from desk research and find an optimal combination between transparency and data protection.

Figure 3: Tokens created by the main account. Screenshot taken after the certificates have been transferred to the student

Table 1: Token structure

Tokenname	Asset ID	Purpose
Apt	15292782904330273875	The approval model is tied to this token. The account that holds this token controls the permissions to send the other tokens.
iccws21a	16499725966910173322	This token is supposed to demonstrate a form of gamification, for example an award token for the best in class. This information is public, but does not

[2] The link to the transaction in the Blockexplorer is https://test.ardorportal.org/transactions/fullHash/a5337c29bfeacc15e96bd4683aa000006e7b74c3ed5de4a6c4c14ccc06cb5868/chain/2

Tokenname	Asset ID	Purpose
		contain any data privacy relevant data within the transaction. This token is sent to the learner.
iccws21m	767675440205673854	This token is sent to the learner. The token contains all relevant metadata regarding the certificate/grade. The message in which the metadata is written is transmitted encrypted.
iccws21s	734472257896719728	The purpose of this token is to transmit an unencrypted message in which only the name of the course and the date or semester is given without disclosing personal data. The transaction number can be used to identify the sender and receiver address. Hereby it can be determined at first sight wheter this is a legitimate certificate (for example, for a quick first check).
iccws21t	10445462519689196681	This token is sent to the teacher. It contains encrypted metadata about the certificate. This data is attached to the token as a message. A special feature of this token is that the metadata no longer needs to be processed by the Blockchain after a predefined time. While the data for the learner is permanently stored on the Blockchain, it is usually only necessary that the teacher only requires a certain period of access to the meta data. If access to metadata is needed beyond this period, this can be arranged via the key of the University through the metadata transaction to the learner.

An important function is the approval model. This guarantees that the tokens are not forwarded to unauthorized persons or even traded on a decentralized stock exchange. With the approval model utilised in this demonstrator, the owner account of the apt token (in this case the University account) must agree to a transaction. This can be done automatically with the first transaction by putting the students' accounts on a permitted list.

The next step involved the simulation that a course has been completed and the tokens were sent from the University address to the student and teacher.[3]

The transaction with the meta data to the student as well as to the teacher was sent encrypted. When the content of the transaction is decrypted, a shared key is generated with which the content can be shared with third parties without having to have a private key.[4] [5] [6]

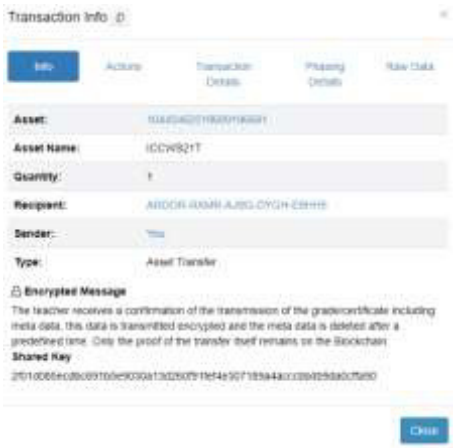


Figure 4: Transaction to the teacher, as encrypted message To complete the list of transactions:

The final step was the creation of a certificate that reflects the Blockchain transactions. This certificate was also connected to the Moodle system of the University. The main advantage is that the identity of the student and the institution is secured in two ways; using Blockchain and the standard e-learning system of the University.

[3] The transaction of the iccws21s token can be viewed at the link: https://test.ardorportal.org/transactions/fullHash/4e4daa67fe34e377849e738264fbf7ba69fd1a4346bf972dc9cede4083619460/chain/2. The text was sent in plain text (unencrypted).
[4] The following is the link to the transaction sent to the teacher: https://test.ardorportal.org/transactions/fullHash/8277be29526077bff0ab9c616fcdec9c672cdd62707f5551530779db3ebd5906/chain/2.
[5] The meta data to the student: https://test.ardorportal.org/transactions/fullHash/2695cfbeb3a871b6c12307f62382dc0516cff8e3a25a4d511b5f27be1f37071f/chain/2
[6] The best student award to the student: https://test.ardorportal.org/transactions/fullHash/2af7f74cfec21fbef8aa4e5fd2a27c9251ce47942f8a0b3b35bc4c092065edf7/chain/2

And even if the University stops operating its e-learning system, the validity of the certificate is still tored on Blockchain, and can be retrieved there as long as at least a few nodes are operated.

Figure 5: Certificate including the respective transfer hashes

5.2 Results of the discussion

The authors will now discuss the results of the focus group, grouped by identified categories.

General judgement

In general, the approach was seen as very innovative. E1 wanted to know how the blockchain processes can be connected to a normal app and the authors explained the possibility of API calls. The structure of the different tokens was highlighted in a very positive way (E2). The fear that no GDPR compliant solution can be developed on Blockchain has been taken away by this demonstration according to E4. The connection with Moodle (a learning management software) was also very well-received. The fact that the exam outcome is traceable even if the University uses a different e-learning system or, for example, the University itself discontinues its operations was positively reviewed (E5).

Chain of Trust and forms of digital identities

E2 remarked that the area of digital identities is an interesting focus of the demonstrator. The discussion revolved around various digital identities that already exist and could be considered. E3 brought into play classic state-issued digital identities, which are assigned by the officially approved trust centres. A further consideration, according to E4, is that identities from social media, such as a verified Twitter account or, as in this example, a Facebook account that can be assigned with a high degree of probability to an institution can be used. E1 advocated a system similar to the one used for issuing SSL certificates, meaning that the ID could also be linked to the URL of an institution. E5 commented on the use of decentralized digital identities. E2, on the other hand, said that social security carriers, banks and companies, which in turn are responsible for checking identities, are also ideal partners for similar projects.

E1 remarked about the importance of establishing where the chain of trust begins. It must be very simple for the user to be able to access such information and this must be continuously identifiable. For Blockchain transactions, E1 has therefore suggested that as a possible improvement, tokens should be sent one after the other in order to be able to include the hash value of the previous transaction. More specifically, in our demonstrator, token iccws21s would be sent first, followed by tokens iccws21m and iccws21t. As such, iccws21m and iccws21t would contain the transaction hash of iccws21s. This would link the tokens with each other. The gamification token iccws21a should have stored the hash value of token 1 as well. This iteration would raise the security and transparency to a new level.

Viewing and understanding the transactions

E3, E4 and E5 were concerned that as non-IT experts they would have problems with the system. They stated that the solutions must be well explained and that there must be a simple user interface. Only when such solutions become user-friendly, these will be accepted. E1 grinned during this statement, but agreed with the IT experts.

Costs involved

E3 noted that every transaction on a public Blockchain carries costs, even if these are small and as such, one has to consider who will bear such costs. In response, E1 mentioned the possibility to combine private and public Blockchains. From time to time the private Blockchain transfers a hash value to the public Blockchain. This implies that the data security can be guaranteed gradually, for example in hourly intervals, and in turn the resulting costs would be very low.

The role of human operators

E2 commented on the fact that fraud can occur even before the data is stored on the secure database. People tend to commit fraud and the school system involves many social processes. E5 referred to recent newspaper articles on this theme, such as the manipulation of SAT scores. However, by digitally securing identities, one might be more cautious about performing frauds. For E1, fraud cannot be prevented but it can be massively reduced. The fact that database entries are no longer simply overwritten, but an account book of the entries is created, the attack vector is much lower.

Cybercrime prevention

A well set up system, like the one presented in this paper, demonstrates that good approaches can technically improve the storage and verification of grades. However, problems can still occur at the intersections, especially if non-secure systems are used, where the grades are stored temporarily or where, for example, e-mail is still used a lot. Regardless of this, the human side previously discussed, will play a major role.

Further aspects to be considered

E5 commented on the ambiguity surrounding the definition of Blockchain. E1 pointed out that there are many different Blockchain systems in existence. E3 even talks about a war within the communities surrounding these terms and types. For E2, the political influence and interference play a major role. E4 has even noted that the current COVID-19 situation, has opened a door for these issues.

6. Conclusion and future research

> *"What Role can Blockchain-based Digital Identities Play to Counteract (Cyber)Crime in Relation to Assessment Results and Credentials in the Educational Sector?"*

Digital identities associated with Blockchain transactions have the potential to limit fraud both in technical terms and in terms of intentional human fraud.

However, there are still some restrictions to be considered:

- There are many different types of digital identities. And one has to be aware of what kind of identity is needed and for what purpose.
- Digital identities can also be stolen or someone can be forced to start a process with one's own digital keys.
- There are different Blockchain systems, each with different advantages and disadvantages, which still need to be evaluated in detail. However, it must ultimately be assumed that there has to be a solution that can interpret different Blockchain systems, both for the institutions and the end-users. Only in this way an international solution will become possible.
- Ultimately it is essential to map a chain of trust transparently and conclusively. There must be no possibility to work with fake accounts. Some approaches from the expert discussion such as the possibility that transactions have to be referenced to each other must be considered for future prototypes. Especially important is how the origin of a chain of trust is identified and which method is suitable. The proposal to

work with domain names on which the SSL certificates are registered was particularly innovative if the digital identity is an institution. But also the possibility to use DID seems to be conclusive and will be considered by the authors in future attempts.

- There is still a lot to be done in the area of awareness-raising for this new technology, for all persons and organizations involved.

Future research processes on this topic must be interdisciplinary. Further prototypes should be tested and evaluated. International cooperation is also essential for research projects, since this topic is relevant far beyond national borders. And finally, the solutions must be applicable internationally.

References

Agustin, F., Aini, Q., Khoirunisa, A., Nabila, E. A. (2020) Utilization of Blockchain Technology for Management E-Certificate Open Journal System. Aptisi Transactions on Management (ATM). 4, 2(Apr2020),134-139. https://doi.org/https://doi.org/10.33050/atm.v4i2.1293.

Atzei, N., Bartoletti, M., Lande, S., & Zunino, R. (2018). A formal model of Bitcoin transactions. Proceedings of the 22nd International Conference on Financial Cryptography and Data Security (FC). Springer.

Baldi, M., et. al. (2019) Security analysis of a Blockchain-based protocol for the certification of academic credentials. arXiv preprint arXiv:1910.04622

Bartolomé, A. & Torlà, C., Castañeda, L., Adell, J. (2017). BLOCKCHAIN IN EDUCATION: INTRODUCTION AND CRITICAL REVIEW OF THE STATE OF THE ART. 61. 10.21556/edutec.2017.61.

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

Lee, S. W., Lee, J. I., Han, D. G. (2013) A study of the threat of forgery of certificates issued online, 2013 47th International Carnahan Conference on Security Technology (ICCST), published by IEEE, Medellin, 2013, pp. 1-5, doi: 10.1109/CCST.2013.6922060.

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

Kalla, A., Hewa, T., Mishra, R. A., Ylianttila, M. and Liyanage, M. (2020) "The Role of Blockchain to Fight Against COVID-19," in IEEE Engineering Management Review, vol. 48, no. 3, pp. 85-96, doi: 10.1109/EMR.2020.3014052.

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

Merija, J., Kapenieks J. (2018) Blockchain and the Future of Digital Learning Credential Assessment and Management. Journal of Teacher Education for Sustainability. 20. 145-156. 10.2478/jtes-2018-0009.

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

Pfeiffer, A., König, N. (2019) Blockchain Technologies and Their Impact on Game-Based Education and Learning Assessment. In: Elmenreich W., Schallegger R., Schniz F., Gabriel S., Pölsterl G., Ruge W. (eds) Savegame. Perspektiven der Game Studies. Springer VS, Wiesbaden

Pfeiffer, A., Thomas, A., Wernbacher T. et. al. (2020) BLOCKCHAIN TECHNOLOGIES IN THE EDUCATIONAL SECTOR: A REFLECTION ON THE TOPIC IN THE MIDDLE OF THE COVID-19 SITUATION. In HS. Mittweida (eds) Konferenzband zum Scientific Track der Blockchain Autumn School 2020, ISSN 1437-7624

Satoshi Nakamoto (2008) Bitcoin: A Peer-to-Peer Electronic Cash System, in Whitepaper online available https://bitcoin.org/bitcoin.pdf (Satashi Nokamoto is a pseudonym, it is not known to the general public who is behind this name.); Accessed: October, 2020

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

Thompson, G., Cook, I. (2014) Manipulating the data: teaching and NAPLAN in the control society, Discourse: Studies in the Cultural Politics of Education, 35:1, 129-142, DOI: 10.1080/01596306.2012.739472

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