

Programme: HN/BSc Computing portfolio

Module: Changemakers: Creativity and Value Creation

Module code: ACCA5033 Contribution to

Overall Module

Assessment (%):

50%

Assignment Title: Assignment 1: Innovation &

Research.

Topic- Analyzing a safe blockchain-supported academic certificate verification model to increase trust, credential fraud and efficiency in verifying credentials in institutions of higher learning

Student Name: FATIMA LO

Student Id:2421636

Date of Submission:05-03-2026

Table of Contents

INTRODUCTION	3
IDEATION & MIND MAP	3
Innovation, Creativity and Value Creation	3
Exploration of Project Concepts	3
Justification of Selected Project.....	4
AIM, OBJECTIVES & RESEARCH AREA	5
Project Aim	5
Project Objectives	5
Research Philosophy	5
Research Strategy and Search Tools.....	6
RESEARCH STRATEGIES.....	6
Validity, Reliability and Ethical Considerations	6
Data Collection Methods and Pilot Study.....	7
Data Analysis Techniques.....	8
REFLECTION	8
Description	8
Feelings	9
Evaluation	9
Analysis.....	9
Conclusion and Action Plan.....	10
OVERALL CONCLUSION	10
REFERENCE.....	12

INTRODUCTION

The high rate of digitalisation of higher education has increased the fears about the fraud of the academic credits, the inefficient validation processes and the validation of the credentials cross the borders. Conventional centralised systems can be easily manipulated, sluggish and costly to administer (Raimundo and Rosário, 2021). Rani et al. (2024) highlight that decentralised and immutable architecture of blockchain technology offers a radical opportunity to increase the levels of trust, transparency and security in credential management. The proposed project will introduce a blockchain-enabled academic certificate verification system as a solution to these systemic issues and generate sustainable institutional value.

IDEATION & MIND MAP

Innovation, Creativity and Value Creation

Innovation has been dominant in the modern society as it is changing the way institutions are run, how people communicate and how trust is built in digital setups. Bhaskar et al. (2021) argue that blockchain within the context of higher education, the growing digitalisation has enhanced access and efficiency, but it has also revealed the vulnerabilities in data integrity and credential verification of the structure. New technologies like blockchain are a transition of centralised power to decentralised trust mechanism, whereby records are stored using a distributed consensus, instead of a single governing authority (Shalini, 2024). The creativity here is associated with reconsidering the old verification systems and creating solutions to address the modern challenges of frauds, cross border mobility and online security. The innovation of trust as a technologically-intelligible aspect as opposed to an institutional presumption can generate quantifiable value in the form of better security, increased efficiency in operations and a boost in the trustworthiness of stakeholders (Lizcano et al., 2020).

Exploration of Project Concepts

There were a number of possible solutions that were put into consideration to tackle the problem of academic certificate fraud and inefficiency. A fraud detection system built by AI might be able to detect red flags in the credential patterns, but these kinds of systems are still reactive and rely on the centralised control of the data (Mohammadi et al., 2019). Another option was to have

a centralised digital verification portal, which would be more accessible, yet would contain a single point of failure and exposure to cyber attacks (Wang et al., 2020). Conversely, a decentralised system that is based on blockchain spreads records to several nodes, a factor that minimises the chances of tampering. Cryptographic hash and immutability of blockchain offer greater integrity protection against traditional databases, in terms of security. Decentralised architectures can enable cross border verification without any single institution as far as scalability is concerned. Additionally, the model of trust is significantly different: the centralised systems need the institutional authority, whereas the blockchain creates the consensus-based validation. This comparative analysis shows that blockchain is more resilient, transparent and long-term once used in credential verification (Pillai et al., 2020).

Justification of Selected Project

The problem of academic certificate fraud is continuing to plague the world and is compromising the credibility of the institutions, as well as causes delays in the verification process by employers and graduates. Manual or centralised digital systems are usually characterized by administration inefficiencies, high operation costs and low border interoperability. Rustemi et al. (2023) emphasise that systemic weaknesses are directly tackled in a blockchain-based framework of verification, which empowers tamper-resistant immediately verifiable credentials. To the students, this increases flexibility and confidence of online qualifications. In the case of universities, it decreases administrative load, including reputational risk (Saleh et al., 2020). The employers enjoy expedited and more viable validation procedures. On the side of economics, automation will save on verification expenses and smoothen the workflow of the institutions. With blockchain, systems can be created where personal data is safe and encrypted identifiers with permission access control can be implemented to achieve authenticity (Rana et al., 2022). This multi-stakeholder impact enables the project to showcase a value creation based on the security, efficiency and responsible digital innovation (Kaneriya and Patel, 2023).

AIM, OBJECTIVES & RESEARCH AREA

Project Aim

This project will focus on designing and critically analyzing a safe blockchain-supported academic certificate verification model that will increase trust, credential fraud and efficiency in verifying credentials in institutions of higher learning. The project aims to gauge the technical strength as well as the functional viability of the adoption of such a decentralised solution in the modern education systems.

Project Objectives

1. To critically examine the existing academic certificate verification systems and find the technical, operational and security constraints.
2. To assess the blockchain technology and smart contract as a safe method of issuing and authenticating digital academic credentials.
3. To develop a conceptual blockchain-based verification system and determine its practicability, ethics and scalability in the context of higher learning.

Research Philosophy

Research philosophy is the system of beliefs with regard to the manner of generating, interpreting and validating knowledge in a study. This project takes a pragmatic research philosophy. Murano et al. (2025) explain that pragmatism focuses on practical problem-solving and it advocates adoption of many approaches in order to attain meaningful results. Since the project aims at designing and testing a technological framework that offers a solution to an actual institutional problem, pragmatism offers leeway to apply a technical analysis alongside stakeholder analysis.

This study is not constrained to quantifiable variables alone, unlike positivism that emphasizes more on objective measurement and hypothesis test. Equally, interpretivism is based on subjective experience and social meaning, which, despite its importance, fails to represent the technical analysis that is needed in the design of a system. Pragmatism enables functional evaluation and situational cognition and thus it is a very appropriate approach in innovation-based research in higher education technology systems (Murano et al., 2025).

Research Strategy and Search Tools

To achieve academic credibility and relevance, a systematic research plan will be used. The peer-reviewed materials will be obtained via such databases as IEEE Xplore, ACM Digital Library, ScienceDirect and Google Scholar. The search terms will be in the form of combinations, i.e. blockchain and academic certificates, digital credential verification and distributed ledger, smart contracts and higher education security. Search results would be refined with the help of the use of the Boolean operators (AND, OR), which would allow making them more precise.

Peer-reviewed journal articles and conference papers that are published within the past eight years will be used as filters in order to ascertain current relevance. Inclusion criteria will be concerned with the studies that will cover blockchain implementation, digital credential systems, or security systems in the educational sphere or other similar areas. Non-academic blogs, opinion writings and publications that are outdated will be disqualified. This is a systematic process which guarantees reliability, relevance and methodological rigour in meeting the research objectives.

RESEARCH STRATEGIES

Validity, Reliability and Ethical Considerations

In order to come up with credible findings, it is necessary to ensure that the methodology used is rigorous. Validity is the degree to which the study is exploring the problem at hand. Validity in this project will be enhanced with the help of the research questions formulated in a clear way corresponding to the given objectives. The interview and survey questions will be formulated in a manner that is measuring the perceptions of trust, security and viability towards blockchain-based credential verification. The research will not be hindered by conceptual inconsistencies because of aligning the aim, objectives and methods that are taken logically (Povse et al., 2023).

This will be done by increasing the reliability of the survey using a standardised survey instrument, which has the same Likert scale questions. Transparency and replication of the research will be possible through clear documentation of the research procedure such as sampling method and data collection steps.

Generalisability will be addressed by selecting the participants who are applicable to the research scenario such as; university students and employers involved in verification of credentials. Even though the research will be conducted at a modest level, the selected population would represent actual stakeholders in the higher education systems.

This research focuses on ethical concerns. Respondents will be involved on a voluntary basis and informed consent will be taken before data is collected. The anonymisation will occur; the storage and processing of responses will be done in compliance with GDPR principles (Pagallo et al., 2018). Another important ethical conflict in the blockchain systems is immutability versus the right to erasure. Although blockchain will guarantee permanence of records, privacy restrictions should be integrated to avoid revealing information about sensitive individual data. It can be seen as a measure of responsible technological assessment.

Data Collection Methods and Pilot Study

This project follows a practical approach, thus the data collection methods are chosen based on its capable ability of informing the system design and its acceptability by the stakeholders. The major process will be an organized online survey to the university students and employers. The use of surveys is suitable since it is possible to collect quantifiable perceptions of trust, usability and security. This is in line with the project objective that seeks to test the feasibility of the project in the context of higher education (Rana et al., 2022).

The survey questionnaire will be conducted on the basis of a five-point Likert scale (including strongly disagree to strongly agree) to determine the attitude towards digital credential verification and the adoption of blockchain. The questions will be based on the perceived reliability, verification speed, the concerns over data privacy and the readiness to implement decentralised systems. During the pilot stage, clarity and relevance will be tested with the help of convenience sampling. Even though this sampling method is not a guarantee of complete representativeness, it is appropriate to preliminarily refine it (Rana et al., 2022).

A pilot survey is going to be done with a small sample of the participants to detect unclear wording or structural problems. The information obtained at this phase will be used to make any amendments like the use of non-technical language or better organization of questions.

Although surveys offer general information, one of its weaknesses is that there would be no detailed qualitative knowledge. This can be dealt with by conducting optional semi-structured interviews with administrative staff members in the university to attach contextual views of implementation issues (Rana et al., 2022).

Data Analysis Techniques

The analysis of quantitative data gathered by the survey will be done by the descriptive statistical analysis. Response distributions will be summarised with the help of frequency tables and the analysis of mean scores will be performed to demonstrate all the general tendencies in the perceptions of the stakeholders regarding trust, efficiency and security. This will enable the researcher to establish the degree to which the participants show their strong support of blockchain-based verification systems (Rouhani and Deters, 2019).

Thematic coding will be used to analyse qualitative data collected through the open-ended survey responses or voluntary interviews. The responses will be classified into common themes like privacy issues, implementation challenges and perceived advantages. A pattern recognition will be used to facilitate further meaning interpretation rather than the numerical outcomes (Rouhani and Deters, 2019).

This analysis is not just meant to report the findings but to update the design. As an example, when the respondents show their concerns about the privacy of the information, the proposed framework may introduce the permissioned access controls or improved encryption. On the same note, the positive feedbacks on the speed of verification can be used to support the feasibility of the system in real life. Connecting the results of the analysis to the project goals directly, the research design makes sure that the results will be applicable in the context of assessing the acceptance of the stakeholders and the viability of the system (Kohad et al., 2020).

REFLECTION

Description

This project was developed due to a general interest in emerging technologies in the higher education sphere. The research and ideation process allowed reducing the scope to academic

certificate fraud and verification inefficiencies. This resulted in the choice of a blockchain-based verification model as a possible solution to systemic trust and security issues.

Feelings

At first, blockchain has been a technical innovation related primarily to cryptocurrency. I was assured in its security capabilities as well as not quite convinced in its practical applicability in education systems. The complexity of implementation was also a matter of some concern as well as whether such a system would be realistically implemented by institutions.

Evaluation

The good thing about this project was that it was well organised in the approach to analyzing the problem and then offer a solution. The consideration of other systems, including centralised databases and AI-based detection tools, enhanced the argument of blockchain adoption. The research work enhanced my knowledge of decentralised trust model and how it may impact society. There were however, difficulties when ethical and legal issues were taken into account. It took more research than expected to understand the compliance with the GDPR and the protection of data in immutable systems. Also, the feasibility preliminary also revealed some practical obstacles like institutional resistance and cost of infrastructure which made what initially seemed to be a simple technological solution more challenging (Shoaib, 2023).

Analysis

This experience showed that the technological innovation is not to be judged only by efficiency or security benefits. I was able to critically identify the moral ambiguity of blockchain systems, especially the conflict between unreliability and the erasure rights under data protection laws. This change in thinking helped me to reconsider my viewpoint on the concept of blockchain as something fundamentally better to look at it as a socio-technical system that needs to be carefully governed. Moreover, increased exposure to academic literature proved that scalability and interoperability defendability are still a current issue in distributed ledger technologies (Reegu et al., 2021). I also understood that technical robustness is not enough in comparison to stakeholder acceptance. Therefore the project broadened my thinking to cover not only technical design but also policy, ethics and organisational behaviour as part of innovation.

Conclusion and Action Plan

To enhance this study in the future, I would consider involving more stakeholders such as policy-makers and IT administrators to have more accurate information on the institutional readiness. I would also consider small-scale technical prototyping in order to test its feasibility in reality conditions. More legal studies of international data protection systems would benefit ethical analysis. This reflective experience has supported the significance of critical thinking and interdisciplinary analysis in designing technology-based solutions in the higher education settings.

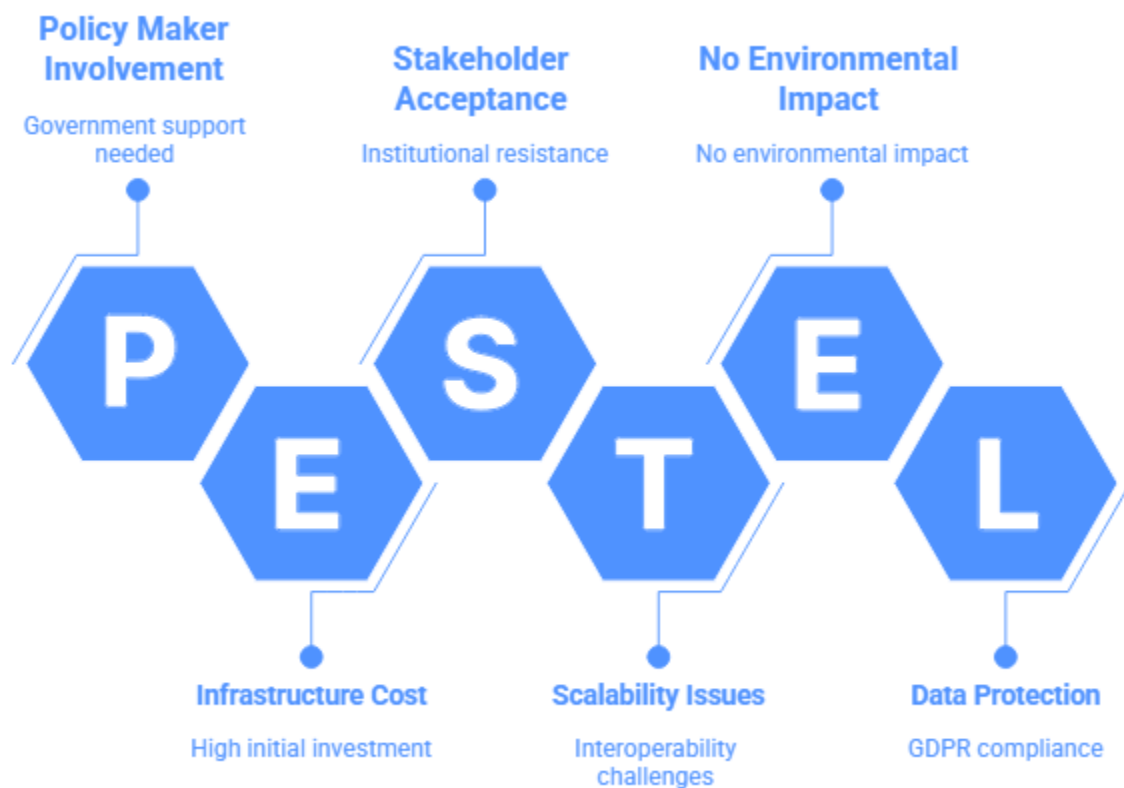


Figure 1: Blockchain in Higher Education

Source: Self Generated

OVERALL CONCLUSION

The given project evidences that blockchain technology can have a great potential to enhance the process of academic certificate verification in the context of higher education. Emphasizing the

aspects of security, trust and efficiency, the suggested framework can help resolve the actual problems, including fraud and delayed validation. Nevertheless, before implementation, ethical, legal and scalability issues should be pondered. All in all, this study has demonstrated that technological innovation should be paired with critical appraisal in a bid to develop viable and accountable solutions to the contemporary education systems.

REFERENCE

- Bhaskar, P., Tiwari, C.K. and Joshi, A., 2021. Blockchain in education management: present and future applications. *Interactive Technology and Smart Education*, 18(1), pp.1-17.
- Kaneriya, J. and Patel, H., 2023. A secure and privacy-preserving student credential verification system using blockchain technology. *International Journal of Information and Education Technology*, 13(8), pp.1251-1260.
- Kohad, H., Kumar, S. and Ambhaikar, A., 2020. Scalability issues of blockchain technology. *Int. J. Eng. Adv. Technol*, 9(3), pp.2385-2391.
- Lizcano, D., Lara, J.A., White, B. and Aljawarneh, S., 2020. Blockchain-based approach to create a model of trust in open and ubiquitous higher education. *Journal of Computing in Higher Education*, 32(1), pp.109-134.
- Mohammadi, V., Rahmani, A.M., Darwesh, A.M. and Sahafi, A., 2019. Trust-based recommendation systems in Internet of Things: a systematic literature review. *Human-centric Computing and Information Sciences*, 9(1), p.21.
- Murano, A., Bruno, B. and Vespri, V., 2025. Blockchain barriers in public organizations: A systematic literature review. *Socio-Economic Planning Sciences*, p.102364.
- Pagallo, U., Bassi, E., Crepaldi, M. and Durante, M., 2018. Chronicle of a Clash Foretold: Blockchains and the GDPR's Right to Erasure. In *Legal Knowledge and Information Systems* (pp. 81-90). Ios Press.
- Pillai, B., Biswas, K. and Muthukkumarasamy, V., 2020. Cross-chain interoperability among blockchain-based systems using transactions. *The Knowledge Engineering Review*, 35, p.e23.
- Povse, D.F., Favenza, A., Frey, D., Mann, Z.Á., Palomares, A., Piatti, L. and Schroers, J., 2023. Data Protection Challenges in Distributed Ledger Technologies: A Combined Legal and Technical Analysis. In *Building Cybersecurity Applications with Blockchain and Smart Contracts* (pp. 127-155). Springer Nature.
- Raimundo, R. and Rosário, A., 2021. Blockchain system in the higher education. *European Journal of Investigation in Health, Psychology and Education*, 11(1), pp.276-293.

- Rana, N.P., Dwivedi, Y.K. and Hughes, D.L., 2022. Analysis of challenges for blockchain adoption within the Indian public sector: an interpretive structural modelling approach. *Information Technology & People*, 35(2), pp.548-576.
- Rani, P., Sachan, R.K. and Kukreja, S., 2024. A systematic study on blockchain technology in education: initiatives, products, applications, benefits, challenges and research direction. *Computing*, 106(2), pp.405-447.
- Reegu, F., Daud, S.M. and Alam, S., 2021. Interoperability challenges in healthcare blockchain system-a systematic. *Annals of RSCB*, 25(4), pp.15487-15499.
- Rouhani, S. and Deters, R., 2019. Security, performance and applications of smart contracts: A systematic survey. *Ieee Access*, 7, pp.50759-50779.
- Rustemi, A., Dalipi, F., Atanasovski, V. and Risteski, A., 2023. A systematic literature review on blockchain-based systems for academic certificate verification. *Ieee Access*, 11, pp.64679-64696.
- Saleh, O.S., Ghazali, O. and Rana, M.E., 2020. Blockchain based framework for educational certificates verification. *Journal of critical reviews*.
- Shalini, P., 2024. Blockchain technology: Architecture, consensus and future trends. *Emperor Journal of Applied Scientific Research*, 6(3).
- Shoaib, B., 2023. The immutable blockchain confronts the unstoppable GDPR. *Seattle J. Tech. Env't & Innovation L.*, 14, p.1.
- Wang, Z., Lin, J., Cai, Q., Wang, Q., Zha, D. and Jing, J., 2020. Blockchain-based certificate transparency and revocation transparency. *IEEE Transactions on Dependable and Secure Computing*, 19(1), pp.681-697.