The Adoption of Blockchain Technology for Developing a Trusted Achievement Record System in Higher Education

Bakri H Awaji

School of Computing
Newcastle University

This dissertation is submitted for the degree of
Doctor of Philosophy

Newcastle University December 2022

I would like to dedicate this thesis to my loving parents, wife, daughters, brothers and sisters.

...

Declaration

I hereby declare that except where specific reference is made to the work of others, the contents of this dissertation are original and have not been submitted in whole or in part for consideration for any other degree or qualification in this, or any other university. This dissertation is my own work and contains nothing which is the outcome of work done in collaboration with others, except as specified in the text and Acknowledgements. This dissertation contains fewer than 65,000 words including appendices, bibliography, footnotes, tables and equations and has fewer than 150 figures.

Bakri H Awaji
December 2022

Acknowledgements

First and foremost, I would like to thank Allah for providing me with the opportunity to complete my research for the PhD studies. Without his blessings, this would not have been possible.

My sincere praises and acknowledgement are to my supervisors: Dr Ellis Solaiman, Prof Lindsay Marshal and Prof Aad van Moorsel for their extraordinary supervision and for giving me the opportunity and support to complete this research and for all their valuable comments, suggestions and many more insights that inspired this work.

Special thanks to Dr Ellis Solaiman who was always there, reviewing my papers very carefully and offering me critical and useful feedback every time I consulted him. Without his great support, I would not be able to complete this research at its current level. I do admire his work attitude and professional skills, and to me, he has been a more than perfect supervisor during my PhD journey.

I would also like to thank my best friend and colleague ever "Adel Albishri" for his support and being a part of my PhD journey; he was there whenever I needed him. Special thanks to my colleague "Aisha Al Arfaj" for her constant support, help, and generosity.

I would also like to thank all of those I have had the pleasure to work with during this research and all participants who contributed to validating the design. In addition, I thank all the participants who answered the questionnaires and others who participated in the evaluation and reviewing process.

I would like to take this opportunity to express my greatest debt to my lovely family, in particular my mother, father, brothers and sisters. Finally, heartfelt thanks go to my wife "Amnah Awaji" and my daughters : "Fatemah", "Yara", "Leen" and "Leena" who have stood behind me and given me huge support during the thesis work.

Abstract

The utilisation of blockchain has moved beyond digital currency to other fields. Regarding education, blockchain applications are relatively new, and the number of products based on blockchain is currently modest. In recent years, the role of blockchain applications in education has received increasing attention across several disciplines, and they have become increasingly involved in education in different ways and forms. However, scant attention has focused on the utilisation of blockchain and smart contracts to create user-friendly infrastructure to record students' achievements in conjunction with a high degree of usability and feasibility.

This thesis primarily introduces a blockchain-based achievement recording system that creates a verifiable record of students' achievements in higher education. The system offers students the opportunity to review their progress, plan for their future accomplishments, and improve their non-academic skills. Furthermore, the knowledge that all of their academic and non-academic achievements will be recorded on a transcript will motivate students to maintain a robust and well-organised record of their work and to perform well in assessments. This trusted system helps to reduce administrative tasks. The benefits of such a system for an employer include producing trustworthy and verified achievement records that have a standardised template to ensure validity which results in benefit to employee.

This thesis explores the subjects and challenges of blockchain-based applications in higher education in a systematic mapping study. Additionally, we investigate the requirements of building a user-friendly blockchain-based trusted achievement record for students in higher education, with the aim of facilitating the verification of their achievements. Consequently, A conceptual design of the system is provided with a profound explanation of its component and usage scenarios, giving information concerning the implementation and verification. Finally, a case study approach is undertaken to collect data from end-users to evaluate the proposed system's usability, feasibility and performance.

Table of contents

List of figures

List of tables

List of Abbreviations

AES Advanced Encryption Standard

API Application Programming Interface

BFT Byzantine Fault Tolerance Consensus protocol

BLOBs Binary Large Objects

BPO Business Process Outsourcing

CAS Content Addressable Storage

CDNs Content Delivery Networks

CVSS Certificate Verifying Support System

CV Curriculum Vitae

DApp Decentralised Application

EOAs Externally Owned Accounts

ETH Ethereum's cryptocurrency (Ether)

EUCS End-User Computing Satisfaction

EVM Ethereum Virtual Machine

HEDD Higher Education Degree Datacheck

IdAM Identity Access Management

IdM Identity Management

IPFS InterPlanetary File System

LRS Learning Record Store

MIT Massachusetts Institute of Technology

NPS Net Promoter Score

P2P Peer to Peer Network

PoS Proof of Stake Consensus protocol

PoW Proof of Work Consensus protocol

RPCA Ripple Protocol Consensus protocol

RRIPEMD Integrity Primitives Evaluation Message Digest

SQL Structured Query Language

SUS System Usability Scale

UI User interface

UX User experience

Chapter 1

Introduction

Every higher education student, for example any individual in tertiary education studying to complete an academic certificate or degree [129], needs to have a university learning record in which their university progress is documented. The system of the higher education adopts a largely unified approach to creating these records and providing official transcripts to validate the student's academic achievements. A student is given proof of their performance through an official university transcript [129]. Official transcripts are important records for determining an individual's employment because they allow potential employers to check their candidate's education. Moreover, employers may evaluate a candidate's skills and suitability for the job by asking them to submit a work portfolio. Research indicates that work opportunities are significantly enhanced through the provision of adequate achievement record (service-based or project-based) [57][123]. Nonetheless, without a reliable achievement-recording framework, it is difficult to guarantee that transcripts or work provided in a portfolio, are completed by the candidate. Thus, reliable learning records can be incredibly valuable. At present, most people use traditional methods when applying for jobs, such as the provision of a Curriculum Vitae (CV). There are a number of online sources that can be used to assist individuals to create CVs and various structures and styles can be employed. Social networking sites including Facebook [1] and LinkedIn [2] can also be valuable platforms when it comes to creating CVs.

To date, no methods have been established that can allow employers to validate the achievements documented in a candidate's CV [26]. Research performed by the Higher Education Degree Datacheck (2021) [58] revealed that about 30% of students and graduates fabricated or exaggerated their skills or academic achievements. NGA HR [3] services are

[1] https://www.facebook.com
[2] https://www.linkedin.com
[3] https://www.ngahr.com/

a well-known human resources Business Process Outsourcing (BPO) company in the UK, published statistics to show that 90% of Human Resource (HR) directors had witnessed exaggerations on a job application [66]. Moreover, there are several factors associated with achievement records and CVs that can cause a lack of trust, [66] one of which is poor data continuity. For the most part, learning data remains static, even if students transfer to a different institution. Each institute has its own independent Learning Record Stores (LRSs), meaning that the new institute cannot analyse detailed data gathered at previous facilities since they only share the final results of student achievements, which leads to a cold-start issue. [66].

Employers and various other authorities have significant concerns regarding the validation of academic certificates for a number of reasons. For example, certain institutions are no longer operational or fail to maintain accurate records. These cases pose significant challenges when it comes to validating the authenticity of educational certificates. More and more institutions are becoming involved in the global education market, which furthers the difficulty of keeping up-to-date with certificate verification [117]. Moreover, a study performed by Han [57] and Vidal [117] showed that, on average, companies spend as much as £40,000 per year to address these issues. Fraudulent achievement records cause major issues for employers and other, honest candidates who are unable to compete with dishonest candidates. It is thus crucial to develop and implement effective measures to prevent certification fraud.

Research performed by NGA (2018) [89] highlighted a number of common areas in which candidates fabricated or lied about the information on the achievement records. The findings confirmed that 44% of candidates for jobs exaggerated or fabricated their achievement information, while 43% lied about their work history. Moreover, 39% of participants lied about their skills qualifications and 32% about their academic qualifications. Additionally, 27% falsified their industry body membership, whilst 24% provided incorrect references [105]. Weak recording, authentication and validation standards of students' non-academic achievements are also a matter of concern because these cannot be verified on official transcripts. Most studies investigating CV fraud have found the topic to have a significant adverse effect on the quality of employee outcomes, which also affects the organization in general in future. [59].

Blockchain technology [57] may play a significant role in addressing the issues outlined above. Blockchain technology's immutability and security have encouraged researchers to investigate its possible usefulness in different fields, including cloud computing, banking, IoT and education. One key advantage of blockchain technology is that smart contracts can be programmed to automate data storage and validation processes [57]. A smart contract can be defined as a self-executed program that can be used in addition to blockchain to create a

distributed application (DApp) that can be used by numerous parties to enhance trust [129]. In Molina-Jimenez et al. [86], the key concepts of smart contracts and their use are discussed in greater detail.

The implementation of a blockchain-based achievement record system would be highly beneficial for students, education institutions and employers as it could enable a verifiable achievements record to be documented. Through this system, students would be able to showcase their achievements to potential employers, which in turn would improve their employability. Moreover, official transcripts enable students to assess their learning progress as well as plan for their future careers. Moreover, knowing that their academic achievements are documented in a transcript can encourage students to work hard and maintain strong work records, which adds further value to their higher education experiences. A trusted and reliable achievement recording system would also benefit the education system itself because it can reduce administrative tasks. It may also improve the quality standards of student admissions by making students' achievements transparent. Moreover, such systems would also have advantages for employers, including the provision of reliable and verified achievement records. It would also enable employers to gain a full, detailed picture of a candidate's higher education achievements, which would be advantageous for the recruitment process [58].

1.1 Research problems

In universities, a paper copy of a final degree certificate which is also stored in the university's database, is awarded to students once they complete their courses. However, despite the built-in security features that paper-based certificates have, there are significant issues regarding the ease with which counterfeit copies can be made. The following issues will be addressed in this work:

1. The higher education system tends to adopt a unified approach when it comes to creating students' achievements records. This typically takes the form of providing official transcripts. Nonetheless, the transcripts only include academic achievements and do not include for students' non-academic activities. However, extra-curricular activities can significantly enhance a student's skills and knowledge. The most significant problem here is the lack of the processes of recording and validating non-academic achievements because such achievements are not contained in any official transcripts. These students are thus unable to provide a proof and comprehensive representation of their achievements during their academic years, including non-academic activi-

ties, voluntary work, roles in student societies and unions, along with employability awards [117] [26].

2. Combatting fraudulent credentials and falsified documents is another significant issue. This can be detrimental to both education systems and society as a whole, as it undermines the value of a university degree and the effort that one makes to be awarded one. Following in the list is the classification of documents fraud and manipulation types within higher education:

   (a) Contents Fraud: Falsified documents can contain various false details, including signatures, references and educational details, as well as false logos and serial numbers. It is also possible for counterfeit documents to be created [105].

   (b) Diploma Mills: A diploma mill can be defined as a company or organisation that officially calls itself a higher education institution, but actually produces illegitimate academic degrees and diplomas for a price. These companies sell false/fake credentials from fictitious universities and currently lead the mass market in achievement fraud. Such organisations are highly structured and sophisticated and operate under a corporate culture with committed marketing and sales teams. Occasionally, they even provide customers with 'tailored' products [59].

   (c) Accreditation Fraud: this is where an accreditation body validating credentials is fictitious or compromised. Many diploma mills choose to establish fake accreditation mills to legitimise the credentials that they sell to their customers [66].

1.2 Aim

This research investigates the feasibility of using blockchain and smart contracts to provide a friendly-use infrastructure for a student's achievement record in higher education that enhances trust, privacy and security. User-friendly means that a software interface that is easy to use and "friendly" to the user, meaning it is not difficult to learn or understand. Consequently, developing a new, reliable system that can be used by stakeholders (for example students, employers and educational organisations) to organise and validate achievement certificates. This system should be accessible to multiple parties (including students, university admission teams and student registration services). Such a system would enable admission staff to assess whether university candidates meet the university requirements without needing to contact certificate issuers for validation. For instance, medical students and employers could

use a system like this to provide evidence of necessary training. What's more, it would allow of verification of information provided on candidates' CVs by employers whilst providing a single, comprehensive record of achievements for students. Moreover, the development of this system would enable educational institutions to deliver a comprehensive picture of students' achievements in their academic and non-academic activities. This system could ensure that CVs and data records are authentic, verifiable, and invulnerable to forgery. The principal aim of this system is to use blockchain and smart contract technology to build an auto-create achievement recording system for students to:

- Record all the activities that student performs during their educational journey.
- Provide proof of students' qualifications and skills that are not recorded in their official academic transcripts.
- Encourage students to earn knowledge from various sources besides academic courses and modules in order to improve their skills.
- Help students to create a future learning plan based on their achievement record.

1.3 Research Questions

To achieve this aim, this thesis addresses the following research questions:

Question 1

How feasible and effective is blockchain technology in implementing a friendly-use trusted achievement record for students in higher education?

As presented in Chapter 3 Section 2.5, a number of applications have been implemented to tackle verifying students' academic documents, as provided in the related work section in chapter two in this thesis. However, in their current formats, to the best of our knowledge, there is a lack of consideration regarding the content requirements, usability and feasibility to design such an application. Therefore, in order to provide a comprehensive answer to this question, we divided this general question into more specific questions as follows:

1. What are the current blockchain applications in higher education? What are their features and limitations?
2. How to determine the requirements for building a blockchain-based achievement record system?

3. How can the documents be verified using blockchain and smart contract technology?
4. How can each user's (students, educators, etc.) operations and transactions be specified in our proposed solution?

Question 2

How can a friendly user-interface be designed and integrated with a smart contract in the blockchain at the back-end?
The aim is to build a homogeneity between the characteristics of blockchain and the operations and transactions at the frontend of the prototype to create an environment for student's achievement records whilst maintaining the security and protection of the data and users' identities. Therefore, in order to provide a comprehensive answer to this question, we divided this general question into more specific questions as follows:

1. What are the modelling scenarios of the system use cases?
2. What are the modelling scenarios of the data flow?
3. How to validate the proposed design?
4. How can we evaluate usability, feasibility, and users' satisfaction with the system?

1.4 Contributions

The first and most important contribution in this thesis is proposing the Blockchain-Based Trusted Achievement Record System designed to be easy to use.The proposed system is a new, trustworthy system that stakeholders (such as students, employers, and educational institutions) can use to organise and validate achievement certificates and other relevant documents. In the following, we summarise the contributions in this research:

- Exploring current research on blockchain-based educational applications through a systematic mapping analysis to collect and analyse important blockchain technology research in higher education. The study focused on two primary themes. First, it searches at the state of the art educational blockchain-based applications. Second, it outlines the research gaps that must be addressed in future studies (**Chapter 3**).
- Conducting a study investigating the requirements to build a blockchain-based achievement recording system. This study aims to collect valuable data from participants that reflect their thoughts and opinions concerning building an achievement recording

system based on blockchain and smart contract technology. The system requirements can be specified once the data has been gathered. This study uses a mixed-methods approach [96]. It involves collecting data quantitatively by way of a questionnaire employing a closed set of questions [97] and a qualitative approach through interviews comprised of open questions and conducted with a number of participants [53] (**Chapter 4**).

- Providing a conceptual design of a Blockchain-Based Trusted Achievement Record System. The tools, components, mechanisms, scenarios, use cases and data flow are presented with a deep explanation as well as the validation process of the design. (**Chapter 5**). In addition, explaining the development of a Blockchain-Based Trusted Achievement Record System. In this stage, the details of converting the system's conceptual design to a software program have been provided. Furthermore, explaining the interactions of end-users with the system (**Chapter 6**).

- Conducting an extensive analysis of the system's usability by adopting the System Usability Scale (SUS) method. This evaluation technique includes a questionnaire that asks users to rate their level of agreement with statements on a number of usability features. (**Chapter 7, Section 2**). Conducting the End-User Computing Satisfaction (EUCS) to determine system satisfaction, conducting a thorough examination of system users' satisfaction. Content, Format, Timeline, Accuracy, and Ease of Use are the five components of end-user satisfaction measured by the EUCS test. A questionnaire containing twelve questions has been sent to participants to measure the five variables. (**Chapter 7, Section 3**).

- Conducting an analysis to assess the system's capability to positively impact the system's users in terms of the motivation to learn, planning for future learning, employment, and providing proof of skills. A qualitative questionnaire has been created to rate the level of agreement with statements covering a variety of objectives that we need to achieve via this system. (**Chapter 7, Section 4**).

- Conducting an extensive analysis of two variables. First, the delay time represents the transaction confirmation time. It refers to the time a transaction takes from its broadcast to the blockchain and addition to the distributed ledger. The second is the cost of the transactions; the cost represents the mining fee (Gas). Gas refers to the unit that measures the computational effort required to execute specific operations on the Ethereum network. Gas fees are paid in Ethereum's native currency, Ether (ETH).

Finally, we surveyed the related work and benchmarked the outcome of our solution with similar solutions in the research area (**Chapter 7, Section 5**).

1.5 List of Publications

Chapters 3, 4, 5, 6 and 7 in this thesis have been published at international conferences and respected journals.The researcher did the whole work, including writing the papers. The co-authors contributed through discussion and revising, editing and providing comments. A list of these publications can be seen below.

Conference Papers:

1. **Bakri Awaji,** and Ellis Solaiman. (2022). **Design, Implementation, and Evaluation of Blockchain-based Trusted Achievement Record System for Students in Higher Education**. In Proceedings of the 14th International Conference on Computer Supported Education **(CSEDU)** - Volume 2, ISBN 978-989-758-562-3, ISSN 2184-5026, pages 225-237. **[Covered in CHAPTERS 5, 6 and 7].**

2. **Bakri Awaji**, and Ellis Solaiman, and Adel Albshri. 2020. **"Blockchain-Based Applications in Higher Education: A Systematic Mapping Study"**. In Proceedings of the 5th International Conference on Information and Education Innovations (ICIEI 2020). **ACM** Association for Computing Machinery, New York, NY, USA, 96–104. DOI:https://doi.org/10.1145/3411681.3411688 **[Covered in CHAPTER 3].**

3. **Bakri Awaji**, and Ellis Solaiman, and Lindsay Marshall. 2020. **"Investigating the Requirements for Building a Blockchain-Based Achievement Record System"**. In Proceedings of the 5th International Conference on Information and Education Innovations (ICIEI 2020). **ACM** Association for Computing Machinery, New York, NY, USA, 56–60. DOI:https://doi.org/10.1145/3411681.3411691 **[Covered in CHAPTER 4].**

4. **Bakri Awaji**, and Ellis Solaiman, and Lindsay Marshall. 2020. **"Blockchain-Based Trusted Achievement Record System Design"**. In Proceedings of the 5th International Conference on Information and Education Innovations (ICIEI 2020). **ACM** Association for Computing Machinery, New York, NY, USA, 96–104. DOI:https://doi.org/10.1145/3411681.3411689 **[Covered in CHAPTER 5].**

Poster:

5. **Bakri Awaji**, and Ellis Solaiman.**"Online Education Using Blockchain and Smart Contracts"**. 11th International Conference on Computer Support Education CSEDU 2019.

Journal: Under Review

6. **Bakri Awaji**, Ellis Solaiman, and Adel Albishri. 2022. **"Blockchain-Based Trusted Achievement Record System"**. **Engineering Reports**, Wiley Online Library.

Furthermore, I am a co-author of some research papers relevant to blockchain and smart contracts, but they do not directly contribute to this thesis. A list of these papers is as follows:

7. Adel Albshri, **Bakri Awaji**, Ali Alzubaidi and Ellis Solaiman. (2022). **"BLOCKCHAIN SIMULATORS: A SYSTEMATIC MAPPING STUDY"**. IEEE SCC 2022 (2022 IEEE International Conference on Services Computing). *[Under Review].*

8. Adel Albshri, **Bakri Awaji**, and Ellis Solaiman. (2022). **"Investigating the Requirement of Building Blockchain Simulator for IoT Applications"**. IEEE SCC 2022 (2022 IEEE International Conference on Services Computing). *[Under Review].*

1.6 Thesis Structure

- **Chapter 2. Background:** Background information about blockchain technology, smart contracts, and smart contracts applications within education has been presented in this chapter. In addition, this chapter explains the methodology employed to conduct the study. Furthermore, this chapter also discusses work related to this study.

- **Chapter 3. Blockchain-based applications in higher education: a systematic mapping study of academic research:** A systematic mapping study was applied to explore the current blockchain applications within higher education systems and identify the gaps for future researchers.

- **Chapter 4. Investigating the requirements for building a blockchain-based achievement record system:** Investigating the requirements for building a blockchain-

based achievement recording system: This chapter introduces two studies, mixed-method approach questionnaire and interview, to identify the requirements to design a blockchain-based system, which produces a verifiable record of achievement.

- **Chapter 5. Blockchain-based trusted achievement record system design:** This chapter mainly introduces the conceptual design of the blockchain-based trusted achievement record system. The tools, components, mechanisms, scenarios, use cases and data flow are presented with an explanation as well as the validation process of the design.

- **Chapter 6. Blockchain-Based Trusted Achievement Record System implementation:** This chapter introduces a Blockchain-Based Trusted Achievement Record System implementation and verification process. This chapter also provided details on converting the system's conceptual design to a software program and explaining end-users' interactions with the system.

- **Chapter 7. Evaluation of the proposed system:** This chapter introduces the evaluation of the system, which includes applying four evaluation methods. These include the System Usability Scale (SUS) [23] to assess the usability of the proposed system and the End-User Computing Satisfaction (EUCS) [65] to evaluate the end-user satisfaction with the system's content, accuracy, format, ease of use and timeliness. This chapter also presents a questionnaire to evaluate users experience (UX) and other research objectives, as well as an analysis of the transactions cost and confirmation time. Finally, it benchmarks the research outcomes compared to outcomes observed in similar projects.

- **Chapter 8. Conclusion:** This chapter summarises the contributions and outcomes of this research, the research limitations and finally, the research's future work.

Chapter 2

Background

Overview

This chapter provides background regarding the technologies, tools and methods related to the research carried out within this thesis. Section 2.1 provides an overview of blockchain definition and platforms. Section 2.2 provides a definition of smart contracts and introduces the structures. Section 2.3 presents the blockchain-based applications architecture , whilst Section 2.4 provides information on the subject of hashing algorithms. he research methodology is explained in detail in section 2.5. Information is provided about the evaluation questionnaires studied in section 2.6. Section 2.7, discusses the blockchain-based solutions made to facilitate the issuance of digital certificates. Finally, concludes the chapter in section 2.8.

2.1 Blockchain Technology

Blockchain is a distributed database that stores the transactions sent between the participants in a secure and immutable way. Blockchain is a P2P network that allows nodes (peers) to collaboratively maintain the network for block and transaction exchange [66]. Figure 2.1

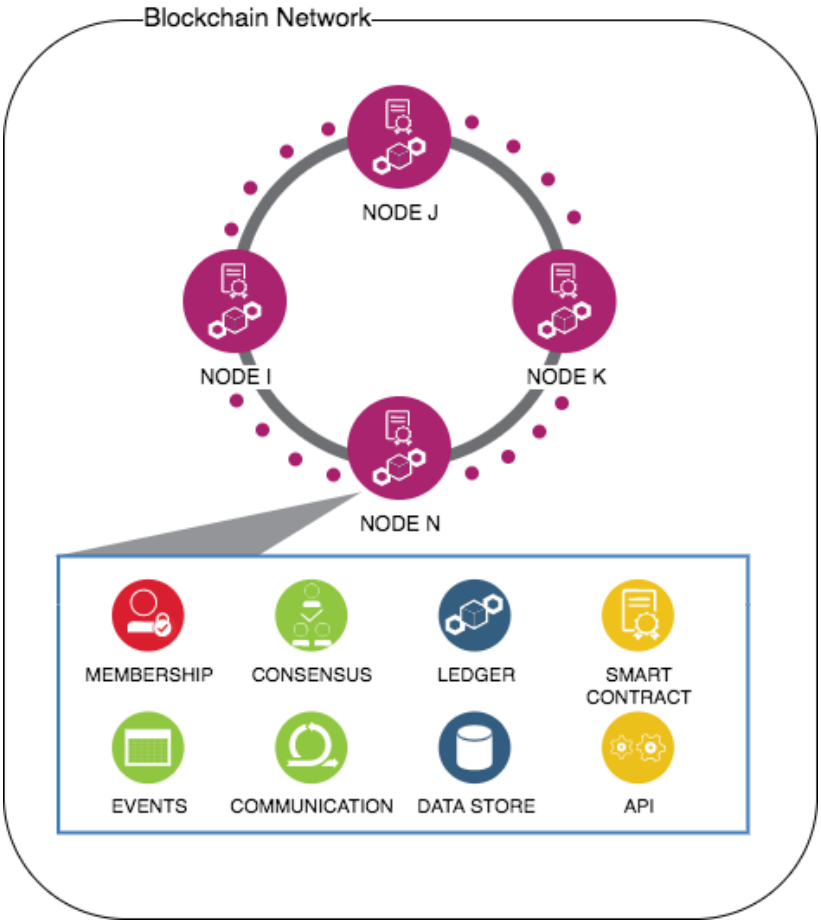


Fig. 2.1 Blockchain Network Overview

shows the main components of blockchain network:

- Membership: unique identities for nodes in the network.
- Consensus: a consensus mechanism is a fault-tolerant mechanism that is used in computer and blockchain systems to achieve the necessary agreement on a single data value or a single state of the network among distributed processes
- Ledger: is a series or chain of blocks on which transaction details are recorded and created after validating the transactions.

- Smart Contract: is a self-executed code that is run to apply roles and conditions between two or more parties
- Events: is an inheritable member of a contract that stores the arguments passed in transaction logs.
- Communication: referred to the fork and read operations used for communication between nodes in the network.
- Data Storage: a private storage on the smart contract where only the contract itself can read, write, modify, and delete data.

There is no need for a third trusted party since the participants can communicate and send transactions between each other directly. Blockchain was first developed for the Bitcoin digital payment system in 2008 [6]. This emerging technology has since grown rapidly and has become the subject of intense research in many industries, research organisations and universities worldwide [9][30][121]. Blockchain aims to solve the problem of a "trusted" central authority taking responsibility for mediating transactions between different parties. Centralisation can result in security problems such as being a single point of failure, as well as other problems such as cost. The decentralised nature of blockchain improves trust between parties in a system and eliminates the need for a trusted third party to perform transactions [25]. As a distributed database, blockchain stores every transaction between the parties. Within a blockchain network, a ledger that maintains a record of all transactions is replicated and shared with all parties.

A cryptographic hash identifies the block and each block references the previous one, which creates a chain of blocks (Figure 2.1). Each block contains several transactions. The maximum size of each block varies according to the blockchain platform type, for example, 1 Mb in Bitcoin and between 20 to 30 Kb in Ethereum [116]. The blocks in the chain are immutable and cannot be changed, which prevents the double-spending problem, which is a potential flaw in a digital cash scheme in which the same single digital token can be spent more than once. [31]. Historically, the first generation of blockchain was cryptocurrency, which is a digital currency based on cryptography and P2P networks. One of the concepts integrated into blockchain is mining, which is the process of adding transaction records to the public ledger of past transactions on the blockchain. The mining process requires a miner on the network to generate the new block of transactions by collecting those transactions into a block, running a mathematical process to verify the block and adding it to the chain of past blocks as shown in Figure 2.2.

The other miners' nodes in the network can validate the newly generated blocks through a consensus algorithm. A second generation of blockchain has emerged in the form of

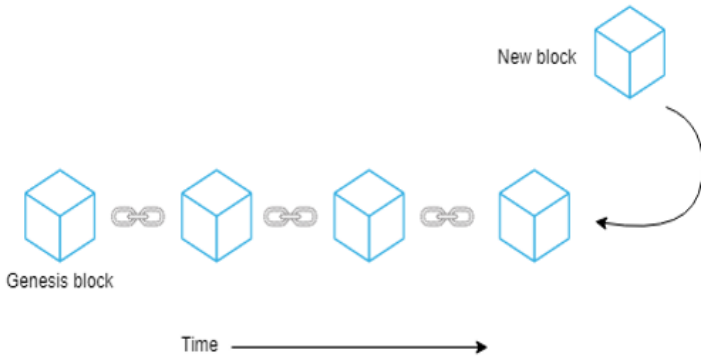


Fig. 2.2 Adding Block to the Chain

Ethereum [30], which allows distributed applications to be built and implemented. Ethereum blockchain allows smart contracts to be built on top of it and consequently, has opened the door for researchers to integrate blockchain into various fields.

Blockchain is also capable of running smart contracts (executable code) [25]. Smart contracts increase the effectiveness of blockchain solutions and allow for distributed applications to be deployed in numerous fields for various purposes. Within the education sector, smart contracts can be used to develop flexible blockchain-based distributed solutions for the benefit of all participants in an online learning system, including students, teaching staff and administrative personnel. For example, it may become possible for students and education institutions to contract more personalised digital agreements which specify assignment requirements, time frames and grading structures [30].

There are a number of blockchain technology features that make it worthy of investigation to enhance educational systems:

- Immutability: the data stored on the blockchain is tamper-proof due to the chronological order that data is stored and the cryptography that secures and connects blocks.
- Reliability: The decentralised nature of the network means that it operates in a more reliable fashion than centralised systems. There is no central authority that could fail.
- Transparency: Transparency of information is an increasing demand. With blockchain technology, it is possible to create highly transparent decentralised data storage.
- Availability: the distributed nature of blockchain infrastructure means that data is replicated, stored closer and accessed more efficiently by owners of the data.
- Trust: Blockchain technology eliminates the need for a trusted third-party service provider to enable communication between parties since the participants can communicate and send transactions between each other directly.

Blockchain has generally been divided into two main types: public and private blockchain [30]. Public blockchain (such as Ethereum [126]) allows anyone to join and participate in the network. In contrast, in a private blockchain (such as Hyperledger Fabric [5]), only users with permissions can join and participate in the network. Finally, the consortium blockchain which includes both private and public blockchain features.

2.1.1 Blockchain Platforms

There are several proposed blockchain platforms in the literature, each with its unique set of features and design decisions [4]. For example, certain platforms (such as Ethereum and Hyperledger) are built expressly to accommodate rich and complicated smart contracts. Table 2.1 shows the most popular platforms of blockchain [62] and their features. Except for Hyperledger and MultiChain, which are platforms for designing and implementing private blockchains, all of these platforms support cryptocurrencies. Based on the objectives of this research, the criteria for selecting the blockchain platform contain two conditions (a. public blockchain, b. support smart contract.). Therefore, the most suitable platform was Ethereum which is the only one in table 2.1 that both conditions apply. More explanation about the chosen blockchain platform provided in Section 2.1.2.

Table 2.1 Characteristics of various platforms of blockchain [4].

	Characteristics			
Platform	Network	Consensus Algorithm	Smart Contract	Cryptocurrency
Bitcoin	Permissionless	PoW	×	×
Ethereum	Permissionless	Pow/PoS	√	×
Zcash	Permissionless	PoW	×	√
Litecoin	Permissionless	PoW	×	×
Dash	Permissionless	PoW	×	√
Peercoin	Permissionless	PoS	×	×
Ripple	Permissionless	RPCA	×	×
Monero	Permissionless	PoW	×	√
MultiChain	Permissionled	Round-Robin	×	×
Hyperledger	Permissionled	PFT/PoS	√	×

Bitcoin [19]. The first and best-known permissionless blockchain network, built as a decentralised cryptocurrency system with no central authority. Bitcoin offers Proof-of-Work PoW; Proof-of-work is the underlying algorithm that sets the difficulty and rules for the work miners do within the Ethereum blockchain; as its consensus technique. PoW is not an

energy-efficient protocol since it necessitates executing computationally costly operations to maintain the blockchain state. Following the popularity of Bitcoin, a slew of other cryptocurrencies have been proposed, some of which use different consensus mechanisms. A consensus mechanism is a fault-tolerant mechanism used to reach the necessary agreement on a single data value or a single state of the network.

Ethereum [126]. A permissionless blockchain platform enables the creation of smart contracts on blockchains. Ethereum uses the Proof-of-Work PoW consensus system for now and intends to change to Proof-of-Stake PoS. As this thesis mainly adopts the Ethereum platform, we discuss it further in this chapter.

Zcash [61]. A permissionless blockchain network that is intended to protect transaction privacy. Zcash uses a zero-knowledge proof mechanism (zk-SNARK) to provide privacy and anonymity to transactions sent to the network. In addition, Zcash employs the exact Proof-of-Work PoW consensus algorithm as Bitcoin.

Litecoin [50]. Litecoin is a digital currency established on Bitcoin but with a few modifications. Litecoin, in comparison to Bitcoin, has a faster confirmation time for transactions than Bitcoin. Litecoin employs the Bitcoin Proof-of-Work system but with the "Scrypt" hash algorithm, which reduces mining centralisation [62]. Domain applications that demand quick transaction and data processing times on a permissionless network may be interested in Litecoin.

Dash [39]. A permissionless blockchain platform that offers a cryptocurrency with privacy protection. Dash, like Bitcoin, secures the network through the PoW protocol. It does, however, strengthen the Bitcoin network by creating a new network tier powered by a set of masternodes. Through "PrivateSend" and "InstantSend," such masternodes provide transaction secrecy and instant transaction validation [113].

Peercoin [134]. A permissionless platform aims to replace the PoW consensus algorithm with PoS. Peercoin was the first platform to propose using the PoS protocol combined with the PoW protocol. [119].

Ripple [7]. A permissionless platform that works as a cryptocurrency and a global financial payment network and uses the Ripple Protocol Consensus Algorithm (RPCA) is a round-based protocol since not every node can become a validator [113].

Monero [88]. A permissionless platform with privacy protection. It is built on the Cryptonote protocol, which includes a ring signature algorithm that conceals the sender and recipient of transactions [80] Monero utilises the Bitcoin Proof-of-Work (PoW) consensus algorithm.

MultiChain [127]. A blockchain platform enables the creation and deployment of permissioned blockchains within and across organisations [13]. For the reason that it

functions in a private and restricted network, MultiChain does not consider computationally costly protocols like PoW. Instead, it uses a round-robin consensus process to determine a set of miners in the network and utilises a parameter called mining diversity to regulate the number of blocks each miner contributes in a given time frame.

Hyperledger [5]. A collaborative open-source project aimed at developing missioned blockchains. Its goal is to create a platform to construct blockchain platforms by providing an infrastructure of diverse modules (such as smart contract engines) and tools. Fabric, Iroha, Sawtooth and Indy are some of the Hyperledger project's versions that have been deployed as missioned blockchain systems. Each of these versions has the same look and feel and a different consensus procedure. For example, fabric [41], the first extendable blockchain technology to support smart contracts, employs the Kafka consensus process.

2.1.2 Ethereum Blockchain

The blockchain platform used for this specific system is Ethereum. Ethereum is an open-source blockchain with smart contract capabilities developed to support the decentralised applications DApp. Moreover, It also supplies a decentralised virtual machine that can complete the necessary scripts through the use of a system of public nodes. This system is considered to be complete, meaning it can recognise other data sets and is also used as the internal transaction pricing mechanism. Those reasons make the Ethereum platform the most appropriate platform for such applications.

Ethereum is one of the most popular public blockchains. Ether is the name applied to Ethereum's currency. Ethereum uses a Turing-complete programming language to handle complex and customised smart contracts. The Ethereum Virtual Machine is where Ethereum smart contracts are executed. Distributed applications can be built with Ethereum utilising high-level programming languages like Vyper and Solidity [126]. This section covers many components of the Ethereum blockchain, including accounts, transactions, blockchains, together with the incentive mechanism. However, we primarily concentrate on the aspects of the work mentioned in this thesis.

Ethereum account. Accounts (users) are classified into externally owned accounts (EOAs) and contract accounts. Each account has a unique address from 160-bit and a balance. Unlike EOAs, contract accounts include a variety of associated code and more storage capacity. In addition, different accounts can communicate with one another via transactions.

Ethereum transactions. Transactions are crucial for maintaining the blockchain's state. Transactions are carried out sequentially in Ethereum. The order of the transactions determines the final state of the blockchain. Transactions are classified into two types: The first one is "transfer" to transfer Ether between accounts. The second is "contract transactions" used to either publish a new smart contract on the Ethereum blockchain or invoke an existing one.
To deploy a new contract, a contract-creation transaction that contains the contract's creation bytecode is published in the blockchain. Then, the contract is deployed and assigned a unique address. Finally, to invoke the contract, a contract-execution transaction is sent to the contract's address, along with the relevant input data.
In Ethereum, transactions are composed of several fields or properties, including the nonce, gas price, gas limit, from, to, value, as well as data. We will briefly describe these characteristics as follows:

- **Nonce:** A counter indicates how many transactions an account has submitted. With each sent transaction, the nonce is increased by one.
- **Gas Price:** The Ethr that the transaction sender pays for each gas unit spent.
- **Gas Limit:** The maximum number of gas units a transaction can consume.
- **From:** The transaction's sender address.
- **To:** The transaction's recipient address.
- **Value:** The amount of currency that will be transferred from an account to another.
- **Data:** The bytecode for creating a new contract or the input data to invoke an existing one.

Ethereum Virtual Machine (EVM). EVM is a stack-based machine responsible for smart contract execution, either contract- creation or contract execution [128] [126]. Each node on the Ethereum blockchain is equipped with a copy of the EVM, enabling it to run contracts. The EVM is comprised of a predefined set of instructions called opcodes. These opcodes are executed sequentially on the EVM. Each opcode that the EVM executes has an associated cost, represented by the unit Gas. The Ethereum Virtual Machine was implemented using a variety of programming languages, including Python, Parity and Go. The Ethereum consensus layer uses the Proof-of-Work (PoW) algorithm with the most extended chain rule to manage possible forks caused by network propagation delays [128].

2.2 Smart Contract

A smart contract is defined as an event–condition–action stateful computer program that is carried out between two or more parties who do not have implicit trust with one another [85]. In other words, it is a self-executed code that is run to apply roles and conditions between two or more parties [25]. Szabo initially proposed the concept of smart contracts in 1994 [112], describing it as "a computerised transaction protocol that executes the terms of a contract." Szabo proposed converting obligations to self-enforcing software code that could be executed without the need for trustworthy third parties. A smart contract can be classified into two categories centralised or decentralised. It can be implemented to run off-chain on a trusted server in a centralised environment or to run on blockchain; via the smart contract that deployed on to of blockchain; in a decentralised environment [85][110]. Figure 2.3 presents the two types of smart contracts.

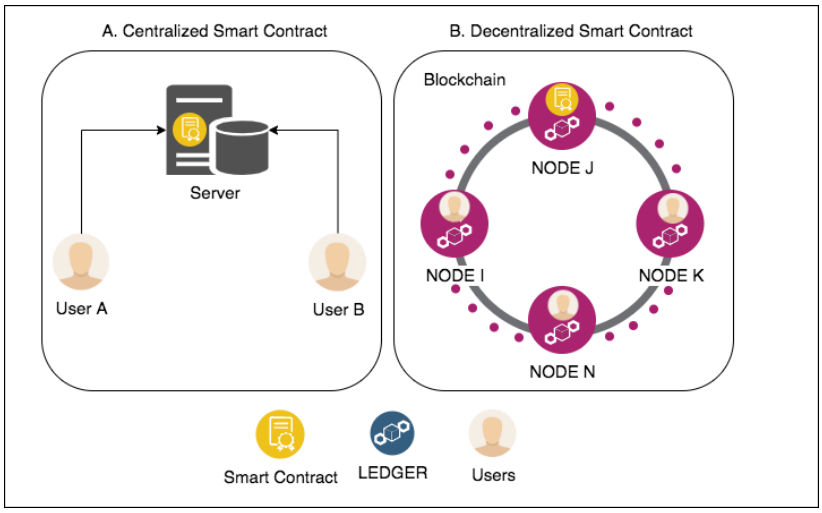


Fig. 2.3 Smart Contract Types

Smart contracts can also be classed as deterministic or non-deterministic on the blockchain. When a deterministic smart contract is executed, it does not require any data from a third party. In contrast, a non-deterministic smart contract relies on data from a third party that is not available on the blockchain. A network of miners manages smart contracts. Miners reach a consensus on the smart contract's execution conclusion and update the blockchain accordingly. Each smart contract is given a unique address and is executed to establish a transaction once deployed. The smart contract's storage can be modified by reading from or writing to it during execution. A smart contract can also use a non-blockchain communication to call and install another smart contract and invoke functions in other smart contracts. Smart contracts can be created on blockchain platforms such as Ethereum and Hyperledger Fabric.

Chapter 3 examines blockchain-based smart contract applications in the field of education, identifying categories of applications, as well as their limitations and gaps.

2.3 Blockchain-Based Applications Architecture

Blockchain technology can be used as a standalone platform to implement complete functionality (via smart contracts) or as an addition to more comprehensive enterprise solutions. Figure 2.4 illustrates the aspect of the three traditional application design types [125].

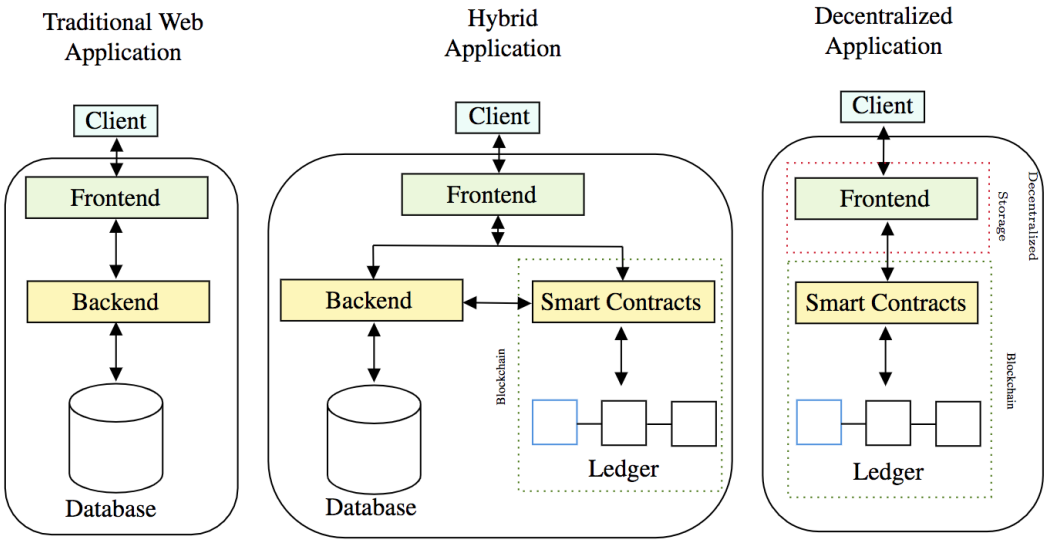


Fig. 2.4 A traditional, hybrid and decentralised application architecture.

- ***Traditional Web (Centralised) Applications:*** Centralised applications are controlled by a single corporation. Information is continuously routed through a single server or cluster of servers in these applications. The dedicated server is equipped with all of the logic necessary to run an application. This also enables it to perform the appropriate action. Since a centralised server controls the applications, the chance of crashing increases. Hence, when the server goes down, the applications stop working across all user devices until the problem is resolved.

- ***Decentralised Applications:*** A decentralised application (DApp) is a type of software created using a distributed computing platform. Typically, a DApp contains a Web interface that communicates directly with a decentralised backend architecture, for example, the blockchain. The frontend code can be hosted on a centralised or decentralised server, for instance, InterPlanetary File System (IPFS) which is a protocol and

peer-to-peer P2P network for storing and sharing data in a distributed file system. The latter achieves complete decentralisation of the application.

- ***Hybrid Applications:*** Developing fully decentralised apps based on distributed components can be challenging. Therefore, this strategy frequently uses a hybrid architecture that incorporates helpful centralised features rather than depending entirely on decentralised features. In this setting, blockchain backend remains vital and various reasons justify its use such its immutability,feasibility and security; even if it reduces confidence in comparison to fully decentralised systems.

2.3.1 Conceptual Components of Blockchain-Based Applications

The fundamental components of blockchain-based applications are consistent across use cases. As a result, we have listed numerous components that every blockchain-like system should consider while designing its architecture. The components' layout patterns are illustrated in Figure 2.5. Such preliminary blueprint patterns might assist with the initial designs and architecture classification for the DApp. We will describe the typical conceptual components of those more extensive design patterns in the sections that follow [125] [124] [118].

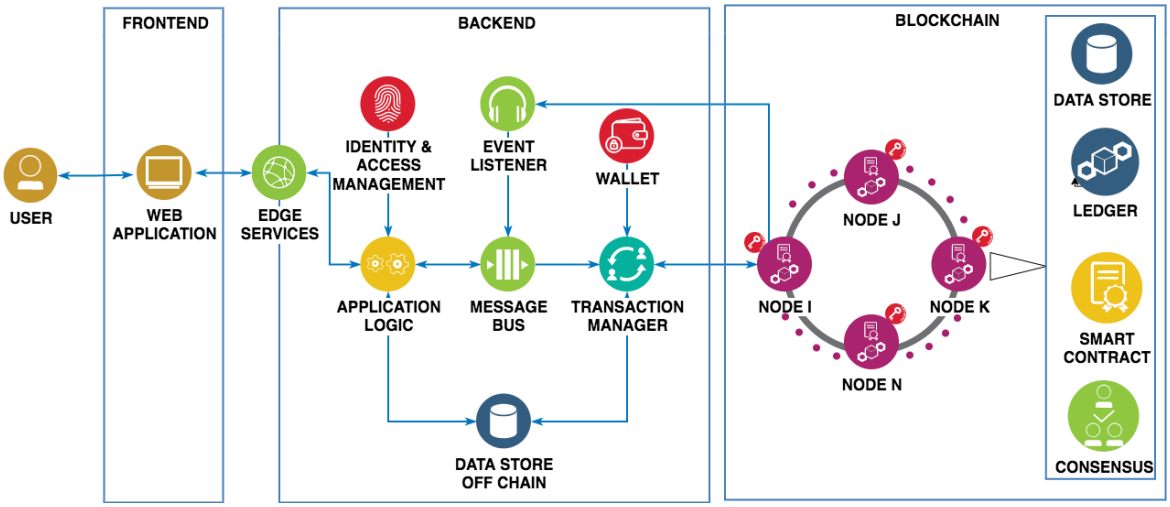


Fig. 2.5 DApp blockchain component structure pattern.

Web Application. A web application is a programme that runs over the Internet and performs activities using web browsers. Most web apps are built in a browser-friendly language like JavaScript or HTML. Because some apps are dynamic, server-side processing is required. A web server is required for a web application to process client requests and carry out the requested operations.

Edge Services. Edge services are components that enable the delivery of content to users via the Internet. The edge services provide various features, including reverse proxies, content delivery networks (CDNs), firewalls, load balancers and API gateways. They usually allow secure data to move from the Internet to the provider's infrastructure and ultimately into the enterprise.

Identity and Access Management. Identity management (IdM), also known as identity and access management (IAM or IdAM), is a set of policies and technologies that enable appropriate users to access technology resources. The identity and access management component maintains user data to authorise users and provide data. It is also used to manage access to resources, services and applications.

Message Bus. The services handle user requests and interact with one another in service-oriented applications. As a result, they must establish an effective communication mechanism. In this case, asynchronous communication via message exchange via a messaging framework has a number of advantages. The messaging framework acts as a message broker, validating, storing (buffering), transforming and routing messages across services.

Off-Chain Storage. Off-chain storage refers to any data stored outside the blockchain. Off-chain storage is necessary for two key reasons. First, to offer speedier access to data stored on blockchain. Second, separate sensitive data from the blockchain for security and scalability. The off-chain storage can take different forms based on the data type and size, for example, SQL, NoSQL for metadata or decentralised Content-Addressable-Storage (CAS) such as IPFS and Swarm for Binary Objects (BLOBs) that generate hashes for data that can be stored on-chain.

Application Logic. An application executes the logic required to accomplish the objectives by creating a monolithic application and a portfolio of services structured to apply mechanisms or scenarios.

Key Vault. A key vault is a component that is used to manage encryption keys. It is critical for giving the private key in circumstances where transactions must be signed in the backend. Numerous intricate methodologies and diverse software solutions enable the secure storage of private keys on the backend, for example, HashiCorp Vault [103] and MetaMask [75]. Certain solutions are based on geographically dispersed databases, while others are built on custom hardware. ***Event Listener.*** Event Listener is a backend infrastructure service that monitors and reacts to events generated on a blockchain side to avoid the direct connection to a blockchain endpoint for events.

Transaction Manager. The transaction manager is a service on blockchain that is responsible for receiving messages and generating state-changing transactions invoking smart contracts. It regulates the way transactions are signed and sent through a connected blockchain endpoint

to the blockchain network. It is also responsible for a variety of tasks related to transactions, such as predicting transaction costs and managing nonces.
Blockchain Endpoint. A Blockchain Endpoint is a node that runs blockchain protocol. Every transaction in each block is checked to ensure network security and data correctness. In section 2.3, we explore blockchain technology in greater depth.
Smart Contract. A smart contract is a self-executing autonomous entity built on the blockchain to carry out operations related to specified tasks. More information regarding smart contracts can be found in section 2.4.

2.4 Hashing Algorithm

A hashing algorithm is a programme that creates a cryptographic hash. It is a mathematical procedure that turns any size data into a fixed-size hash [52]. A hash function algorithm is designed to be a one-way function that is computationally impractical to invert. This thesis primarily focuses on the SHA-256 algorithm, which we discuss in further detail. Standard hashing algorithms include the following:

MD5. Ronald Rivest created it in 1991 [101]. The MD5 method was one of the first to acquire widespread recognition, and it was thought to be secure at the time. However, the MD5 hash function can now be inverted. As a result, it can no longer be used.

RIPEMD-160. Hans Dobbertin developed the RRIPEMD (RACE Integrity Primitives Evaluation Message Digest) cryptographic hash technique in 1996 [36]. RIPEMD was built with the same structure concepts as MD4 while it performs the same function as SHA-1.

Whirlpool. Whirlpool is a cryptographic hash method developed by Vincent Rijmen in 2000 [14] based on a significantly modified version of the Advanced Encryption Standard (AES) to provide a hash digest of 64 bytes.

BLAKE2. BLAKE2, an upgraded version of BLAKE, was released in 2012 [10]. Philippe Aumasson created it to replace the broken MD5 and SHA-1 algorithms. When performed on 64-bit x64 and ARM CPUs, BLAKE2b outperforms SHA-3, SHA-2, SHA-1, and MD5. BLAKE and BLAKE2 are, however, not as widely used as SHA-3. As a result, BLAKE was proposed as a successor for SHA-3.

SHA. The US government designed the early versions; other programmers have modi-

fied the core frameworks and generated additional sufficiently rigorous iterations and tough to breach. The higher the number after "SHA," the more recent and complicated the release. Thus, it became a common hashing method in 2015 [51]. As a result, it was adopted as a standard hashing method in 2015 [51]. However, following a series of successful attacks, the big three – Microsoft, Google, and Mozilla – discontinued support for SHA-1 SSL certificates in their browsers in 2017 [51]. SHA-2, on the other hand, contains a slew of substantial changes. Its family consists of six hash functions with digest lengths of 224, 256, or 512 bits.

SHA-3 was created by Guido Bertoni. SHA-3 is more resistant to attacks and much faster than SHA-2. This is due to the "sponge construction." Data is "absorbed" by the "sponge" and then "squeezed" out, resulting in the hash [51]. When using SHA-256, there are 2256 potential hash values, making it impossible for two different documents to have the same hash result. In contrast to some other common hashing methods, SHA-256 is secured and has not been broken. As a result, we used it in our proposed system.

2.5 Related Work

Recently, blockchain and smart contracts applications in education have gotten attention, increasing the utilisation of this innovation within the education field. However, blockchains in education are primarily utilised to record grades and award certificates; far, little attention has been given to the utilisation of blockchains and smart contracts to build infrastructure for students' learning achievement [9]. The following is the current blockchain and smart contract applications categories within the education field:

- Digital certificate applications: the key aim of these applications is to control the students' earned academic achievements and facilitate storing, verifying, and validating credentials. Examples are Open Blockchain [30] and the Blockcerts projects [33].
- Support services applications: These applications are aimed at specifying a cryptocurrency based on Bitcoin to control services in the education area. Examples of these services are support services, enrolling in online courses and training. An example is Edgecoin [94].
- Earnings applications: Learning and earning are linked in these applications. The teaching or learning hours are stored on the blockchain. An example is the Ledger project [126].

Issuing paper certificates requires many manual processes and consumes countless resources, effort and time. Moreover, the probability of errors, forgery or manipulation is also

high. To overcome the limitations of paper certificates, numerous proposals have been made to automate and simplify the issuance of digitised physical certificates. Meanwhile, saving the digital certificates in different locations resolves the issue of them being lost or destroyed.

However, digital certificates still have transparency, dependency and trust issues [90]. Furthermore, significant expenditure and the consumption of human resources are issues associated with the authentication of certifications, due to the rules and procedures currently in place. One instance of this is how the accuracy of certificates needs to be confirmed through a service provided by the entity that issued the certificate. Given that this is a procedure completed by hand in the case of physical certificates, expenditure and time are both consumed by the validation procedure.

Additionally, it is feasible that conspiracy to deceive may be agreed between an individual receiving the certificate and the individual providing validation, while official certificates' inclusion of misleading information is an existing challenge. A second example is how the issuer of the certificate is the sole entity that holds the original and confidential data relating to the certificate holder, meaning that their certificates cannot be confirmed by third parties such as employers. Rather, confirmation must be sought from the issuing entity, which can take time. It is also apparent that the certificates presented by applicants do not provide a straightforward indication of their abilities to the prospective employer. Consequently, the entities issuing certificates may be perceived inaccurately and negatively by recruiters.

Several resolutions have been suggested and implemented in response to the highlighted issues. For example, physical certificates have been supplanted by numerous organisations internationally through the adoption of Open Badges, a Mozilla program. The production, issuance, accessing and authentication of digital certificates are all possible through Open Badges that is using Blockchain technology [63].

Open Badges [63] creates a wallet for the recipient of a certificate, with the certificate accessible from this wallet once Open Badges has been used to create a certificate. The entity issuing the certificate will have provided authentication of it automatically via the wallet before it becomes available. The certificate's inclusion in the wallet's retained record only occurs once the legal authentication procedure has been successfully completed. Therefore, the wallet's certificate list provides veracity for all entities and individuals. Fundamentally, issues such as damaged or misplaced physical certificates, as well as their associated management and printing expenditure both financially and time-wise, have been tackled through Open Badges. Nevertheless, prospective single-point failures in the service or Open Badges database pose safety, security, dependability and transparency issues relating to the platform's management of the issued certificate database. Consequently, entities, particularly

state institutions that feel they lack control over the database provided by Open Badges have shown reluctance and scepticism over the platform's adoption [63].

Blockcerts [106] [64] an alternative program for the issuing and validation of certificates that relies on Blockchain is a cutting-edge, Massachusetts Institute of Technology (MIT) project [106]. Blockchain can be used to develop programs to issue and validate certificates by means of Blockcerts, which comprises decentralised and open mobile applications, tools and databases. Various documents, including practice permits, education certificates or criminal records, can all be incorporated. Despite the issuer of the certificate and any other entity not being involved in the validation process, the certificates' dependability is still guaranteed by Blockcerts. Moreover, if Bitcoin continues to exist, then single-point failures will not be a problem, according to Blockcerts. As a result, continuous accessibility and executability of Blockcerts' services have been achieved. Users activities are entirely their own responsibility because complete user privacy is promoted by Blockcerts. One example is how certificate issuance is permitted solely by issuing entities. The issuing entity and the owner of the certificate both have to consent to a certificate's rescindment, with the irrefutability of such activities being ensured. The certificate is represented by the transactions managed by every Bitcoin address, meaning that a straightforward process is offered by Blockcerts. Accordingly, customers may be persuaded to adopt the program, while its openness is also enhanced. Additionally, mobile software may be used to undertake every certificate management function. Nevertheless, the implementation of Blockcerts is confronted with a number of difficulties [107].

CVSS [90] Blockchainised Certificate Verifying Support System (CVSS) deployed by Vietnam's Centre of Computer Engineering, HCMC University of Technology. This approach utilises blockchain technology to issue immutable digital certificates and improve the current limitations of the existing certificate verifying systems in Vietnam. This project has run a number of short-term modules that adopted the CVSS to evaluate the proposed solution. The CVSS system needs to educate users regarding blockchain in order to use it, which is one of the system's limitations.

CVTrust [69], Smart Diploma [42], cvtrust-efmd [55] as well as **Block.co [18]** are further applications that engage in certificate issuance and validation on the basis of Blockchain. Nevertheless, their adoption approach and technical resolutions are not thoroughly clarified by these systems.

This study's devised system is contrasted with some of the existing Blockchain-based systems employed for certificate validation in Table 2.2,with their principal shared characteristics also presented. Notably, the character of the entity pursuing the system's implementation, for example, academic institutions, will shape the aims informing the development of the particular system.

Table 2.2 illustrates the features of the existing Blockchain-based systems employed for certificate validation. The comparison between those systems is focused on the main features such as accreditation, verification, privacy, transparency, User experience and sharing records. The privacy, accreditation and User experience features are considered as central parts of all current solutions The privacy, accreditation and User experience features are considered central parts of all current solutions, while the other features are added based on the system objectives.However, the proposed solution in this research mainly covers all the necessary features, as shown in Table 2.2. Moreover, as a means of increasing the reliability of our proposed system, we appraised it by applying various reliable evaluation methods. As is apparent from Table 2.3, the most related systems concentrated primarily on analysing user experience. Conversely, in our proposed approach, we focused on assessing more comprehensive aspects to ensure our proposed system's quality while also improving its suitability for the end-user. The user experience evaluation method in similar systems is not clarified in the table below. However, in our proposed system, the user experience was evaluated by collecting and analysing data from real users of the system. Participants comprehensively tested the system and then responded carefully to the two questionnaires designed to evaluate the end-user experience. As a result, our proposed system offers greater reliability in that its effectiveness has been appraised on the basis of different methods as follows:

- A System Usability Scale (SUS) [23] to evaluate system usability.
- An End-User Computing Satisfaction (EUCS) [1] to evaluate end-user satisfaction according to the system's content, format, accuracy, timeline, as well as easy to use.
- Mixed-method questionnaires to evaluate the user's experience (UX).
- Collection and analysis of data from the 'etherscan.io ' tool, as a means of evaluating transaction cost and transaction confirmation time.

The CVSS system is the only system that conducts financial analytic transactions and explains the transaction cost while also providing the transactions' confirmation time on the Ethereum blockchain. Therefore, we compared the financial analysis of our system with the CVSS system in Table 2.3. The evaluation section in (Chapter 7, Section 5) provides an

extensive explanation of this point. However, all the applications and solutions explained above are not open sources, and the system components and tools are not clearly defined.

Table 2.2 Summary Comparison of Various Solutions.

	Features					
	Accreditation	VERIFICATION	PRIVACY	Transparency	USER EXPERIENCE	Accessibility	Sharing Record
OpenBadges	●	⊗	●	⊘	●	●	⊗
Blockcerts	⊗	●	●	●	●	●	●
BLOCK.CO	●	●	●	⊗	●	●	⊗
SMART DIPLOMA	⊗	●	●	⊗	●	●	⊗
CVTRUST	⊗	⊗	●	⊘	●	●	⊘
CVSS	●	●	●	●	●	●	⊗
OUR SYSTEM	●	●	●	●	●	●	●

⊘= Partially Provided ●= Provided ⊗= Unprovided

Table 2.3 Comparison of Various Systems' Evaluation Methods.

	Evaluation Methods				
	System Usability Scale (SUS)	End-User Computing Satisfactory (EUCS)	Use Experience (UX)	Transaction Cost	Confirmation Time
OpenBadges*	⊗	⊗	•	⊗	⊗
Blockcerts*	⊗	⊗	•	⊗	⊗
BLOCK.CO*	⊗	⊗	•	⊗	⊗
SMART DIPLOMA*	⊗	⊗	•	⊗	⊗
CVTRUST*	⊗	⊗	•	⊗	⊗
CVSS*	⊗	⊗	•	•	•
OUR SYSTEM*	•	•	•	•	•
* Has End-User Tool	•= Provided	⊗= Unprovided			

2.6 Research Methodology

The methodology section provides a clear explanation of the strategies and studies applied to answer the research questions listed in chapter 1, page 5. A comprehensive review of the technology, systematic mapping study and system component investigation study were taken to understand how to develop a decentralised software application based on blockchain and smart contract technology to record students' achievements in higher education; steps 1,2 and 3 in figure 2.6.

The literature review in step 1, and systematic mapping study in step 2 define the problem and narrow the research focus. An in-depth review of the technology adopted in this thesis is conducted in the literature review to understand and find the best way to involve them in designing the proposed solution. The systematic mapping study is conducted to determine current solutions and their limitations that future researchers should address. The outcome of these studies defines the research questions that will be answered in this thesis.

Subsequently, a mixed-method questionnaire and interviews in step 3 are conducted to collect valuable data to determine the proposed solution components and tools. This study asks how to choose the requirements for building a blockchain-based achievement record system. How can we verify the documents using blockchain and smart contract technology, and how will each user's (students, educators, etc.) operations and transactions be specified in our proposed solution? Next, based on the analysis of the results of the studies conducted above, the model conceptualisation design of the proposed solution is built, step 4 and then validated through a focus group workshop with experts. Once the conceptualisation model is validated, the system will be implemented n steps 5, 6 and 7, verified and tested.

The proposed solution will be evaluated, step 9, through an experiment that covers all the evaluation methods relevant to the research aim and objectives. In particular, we assess the system usability via the System Usability Score (SUS) test; block10. Also, we evaluate the satisfaction of the system users using the End User Computing Satisfaction (EUCS) test; step 11. Furthermore, the evaluation of the system's feasibility via a mixed-method questionnaire; step 12. Finally, conducting a performance evaluation; step 12; and comparing the results to the current solutions. The strategies mentioned above are outlined in 2.6 and defined with more details below:

Defining the problem.

Defining the problem in order to identify the aim, research questions and objectives. This task entails conducting a literature review identifying research gaps and identifying future research directions. Additionally, we will narrow the topic of interest by looking for specific keywords and phrases, resulting in explicit knowledge of the previous studies' strengths and shortcomings.

Defining the requirements. After a problem specification, a systematic mapping study was used in this stage to collect information about the current blockchian-based applications within higher education. The study focused on two primary themes. First, it searches at the state of the art educational blockchain-based applications. Second, it outlines the research gaps that must be addressed in future studies (**Chapter 3**). This study outcomes provide an answer to the first research question 1.3.
An investigation study conducted defining the software functionality and requirements needed for a blockchain-based achievement record system prototype. This study aims to collect valuable data from participants that reflect their thoughts and opinions concerning building an achievement recording system based on blockchain and smart contract technology. The system requirements can be specified once the data has been gathered. This study uses a mixed-methods approach [96]. It involves collecting data quantitatively by way of a questionnaire employing a closed set of questions [97] and a qualitative approach through interviews comprised of open questions and conducted with a number of participants [53] (**Chapter 4**). This study outcomes provide an answer to the first research question 1.3.

Model conceptualisation. In this step, we will develop a software model (i.e. a model for the prototype software) that accurately represents the real system. The primary aim of this model is to reflect the software components and use cases to demonstrate the ensuing outputs. Therefore, we will exclude unnecessary features and focus exclusively on the primary purpose to maintain the model's realistic complexity. The tools, components, mechanisms, scenarios, use cases and data flow are presented with a deep explanation as well as the validation process of the design (**Chapter 5**). This study outcomes provide an answer to the second research question 1.3

Design Validation. Design Validation is the process of ensuring that a prototype meets the requirements of its users. Design validation verifies that the prototype design meets the criteria for implementation for the users. If the model is determined to be invalid, the

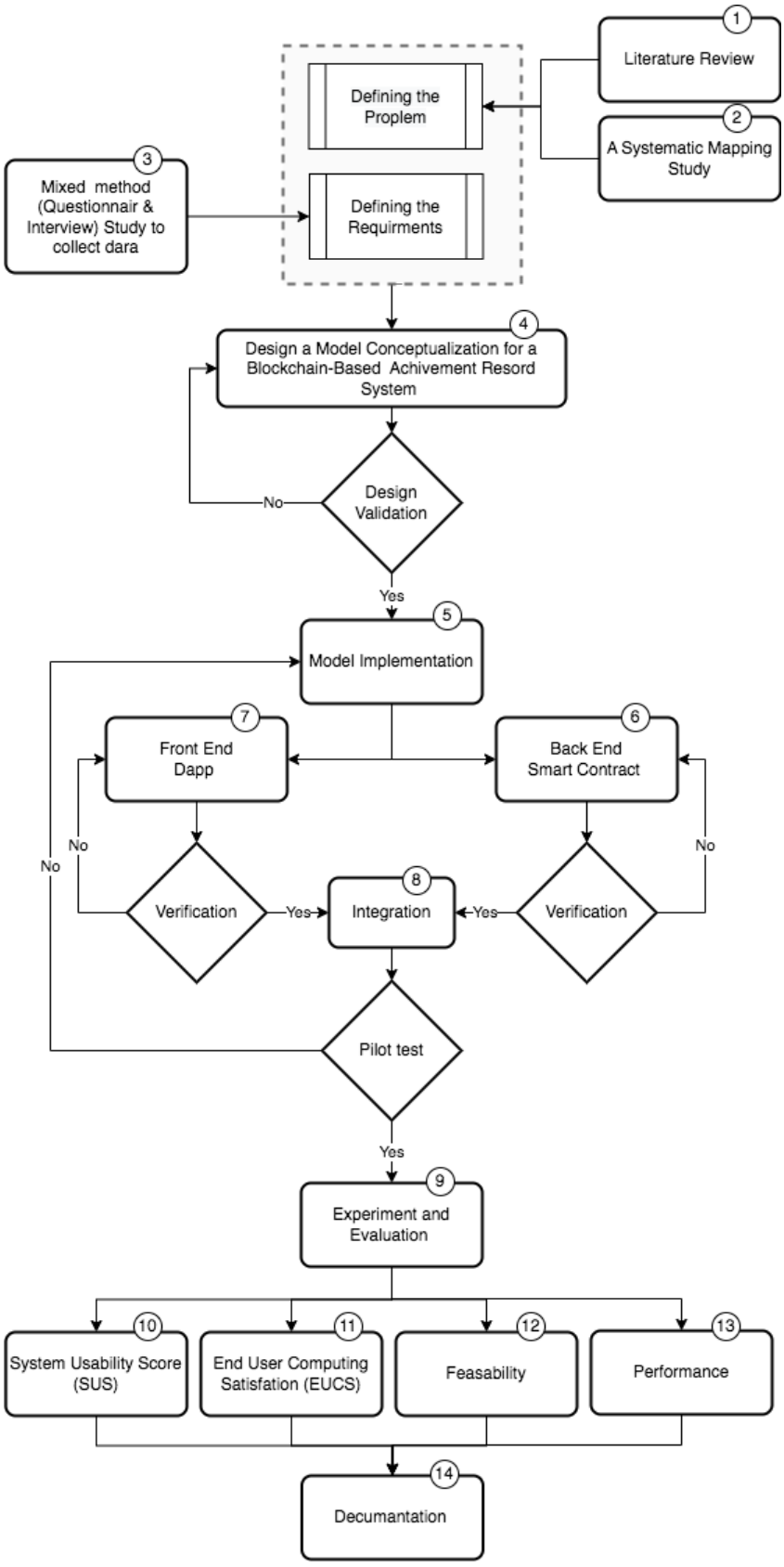


Fig. 2.6 Research Methodology.

modeller should change the model's design, model assumptions and data gathering procedure. The validation process starts together with the conceptualisation of the model and continues until the model is successfully translated into a program.

Model implementation. The primary aim of this stage is to convert the conceptual model developed in the previous step into a software system. The implementation is a two-sided process. We will concentrate on the design of the smart contract and its deployment on the Ethereum blockchain on the one side and the development of the decentralised application on the other. (**Chapter 6**).

Implementation verification. This stage verifies that the conceptual model has been implemented correctly. That is, the verification stage is a debugging task that primarily guarantees the prototype program is free of errors and capable of performing the functions specified in the model. Following the implementation of each component of the model, the verification process is used to identify and correct errors in the early phases. After implementing the entire model, the prototype software must be verified. This study outcomes provide an answer to the second research question 1.3

Integration. Integration is the process of bringing together the two sides of implemented sides of the prototype to create a unified single system. In this step we ensure the front-end is presenting the smart contract functionalities as well as the off chain functions based on the prototype's conceptualisation design.

Pilot test. Pilot testing is a type of software testing in which a small group of users employs the software in its entirety before the software's final launch or deployment [32]. This type of testing verifies the operation of a system component or the entire system in a real-world operational environment.

Usage Experiments. This step is predominantly dedicated to using the prototype by real end-users and reporting their experiences in order to evaluate the objectives of this research study. This involves defining the conditions, mechanism and scenarios to be run.

Evaluation. Upon obtaining the results of the previous step, we can evaluate the proposed system to achieve the research objectives. This study outcomes provide an answer to the second research question 1.3.

Following are the evaluation methods conducted in this research:

- Conducting an extensive analysis of the system's usability by adopting the System Usability Scale (SUS) method [23]. This evaluation technique includes a questionnaire that asks users to rate their level of agreement with statements on a number of usability features. (**Chapter 7, Section 2**).
- Conducting the End-User Computing Satisfaction (EUCS) [65] to determine system satisfaction, conducting a thorough examination of system users' satisfaction. Content, Format, Timeline, Accuracy, and Ease of Use are the five components of end-user satisfaction measured by the EUCS test. A questionnaire containing twelve questions has been sent to participants to measure the five variables. (**Chapter 7, Section 3**).
- Conducting an analysis to assess the system's capability to positively impact the system's users in terms of the motivation to learn, planning for future learning, employment, and providing proof of skills. A qualitative questionnaire has been created to rate the level of agreement with statements covering a variety of objectives that we need to achieve via this system. (**Chapter 7, Section 4**).
- Conducting an extensive analysis of two variables. First, the delay time represents the transaction confirmation time. It refers to the time a transaction takes from its broadcast to the blockchain and addition to the distributed ledger. The second is the cost of the transactions; the cost represents the mining fee (Gas). Gas refers to the unit that measures the computational effort required to execute specific operations on the Ethereum network. Gas fees are paid in Ethereum's native currency, Ether (ETH). Finally, we surveyed the related work and benchmarked the outcome of our solution with similar solutions in the research area (**Chapter 7, Section 5**).

Documentation and Reporting. This step is primarily dedicated to documenting the outcomes of the research study. All the results will be documented, with conclusions, limitations and future work.

2.6.1 Data Collection Methods

In this section, we first discuss the data collection methods conducted in this research to measure usability, effectiveness, performance and cost of the proposed system.

System Usability Scale (SUS).

In 1996, John Brooke described the System Usability Scale, as a "quick and dirty" unidimensional usability scale (SUS). The SUS was created in response to a lack of cost-effective or feasible alternatives to conduct a comprehensive context usability analysis [23]. Brooke presented a quantitative method for assessing perceived usefulness that required less work and expenditure than other methods. It is concise, consisting of ten statements on a five-point Likert scale ranging from strong disagreement (1) to strong agreement (5) [20].

The items are brief statements such as "I believed the system was simple to use." They were created to enable responders to express potentially high levels of agreement or disagreement. The scale alternates between positive and negative items to correct for biases introduced by inattentiveness during completion. The final grade is calculated on a scale of 0 to 100. When compared to other usability scales such as the Questionnaire for User Interface Satisfaction (QUIS) and the Computer System Usability Questionnaire (CSUQ), this simple scale was proven to be more trustworthy across a range of sample sizes [23].

The SUS has become an industry standard. Among the highlighted advantages of using SUS is that it is a simple scale to administer to participants. It is also capable of producing solid results with small sample sizes. It is a valid method for distinguishing between usable and unusable systems.

When the SUS is employed, participants are asked to rate the following ten questions on a scale of Strongly Agree to Strongly Disagree using one of five responses:

1. I think that I would like to use this system frequently.
2. I found the system unnecessarily complex.
3. I thought the system was easy to use.
4. I think that I would need the support of a technical person to be able to use this system.
5. I found the various functions in this system were well integrated.
6. I thought there was too much inconsistency in this system.
7. I would imagine that most people would learn to use this system very quickly.
8. I found the system very cumbersome to use.
9. I felt very confident using the system.
10. I needed to learn a lot of things before I could get going with this system.

Calculating the SUS Scale. To calculate the System Usability Score (SUS) we apply the following steps:

- First, we calculate the average for each Likert Scale question in the test:

$$\text{Avg} = \frac{Number\,of\,answers}{Total\,number\,of\,participants} \times 100 \tag{2.1}$$

- Second, we calculate the weighted average for each question:

$$\text{Weighted Average} = \frac{\sum_{i=1}^{n=5} Avg_i}{n} \tag{2.2}$$

n is the number of answers seen in the Likert Scale

- The third step, we calculate X; which is the sum of the odd questions only:

$$\text{x} = \sum_{n}^{1} Avg\,Odd\,Questions \tag{2.3}$$

- The fourth step, we calculate Y; which is the sum of the even questions only:

$$\text{Y} = \sum_{n}^{1} Avg\,Even\,Questions \tag{2.4}$$

- Next, we calculate XO; which is the sum of odd questions - 5:

$$X0 = X - 5 \tag{2.5}$$

- Next, we calculate YO; which is 25 - the sum of even questions:

$$Y0 = 25 - Y \tag{2.6}$$

- The last step, we calculate the SUS score:

$$SUS = (X0 + Y0) \times 2.5 \tag{2.7}$$

Interpreting the Score. The participant's scores for each question are transformed to a new number, summed together and then multiplied by 2.5 to convert the participant's original 0-40 scores to 0-100. While the scores range from 0 to 100, they are not percentages and

should be considered in terms of their percentile ranking only. For example, a SUS score of greater than 68 is considered above average, according to studies. Conversely, anything less than 68 is below average. Figure 2.7 represent the associated categories with the SUS score in terms of Grades, Adjectives, Acceptability and Net Promoter Score (NPS). The grades are presented in the five letters A, B, C, D, and F. Each of the letters covers a range of scores on the scale, as well as the adjectives that are also classified into six categories starting from the Worst Imaginations and ending with Best Imaginations. Regarding the acceptability, if the sus score is between 0 and 50, then the system is considered "Not Acceptable", and it is considered "Marginal" if the sus score is between 51 to 70. On the other hand, a sus score above 71 is regarded as an "Acceptable". Finally, the Net Promoter Score NPS is classified into three categories Detractor, Passive and Promoter. Detractor if the sus score is between 0 to 60, Passive if the sus score is between 61 to 80, Promoter if the sus score is above 81.

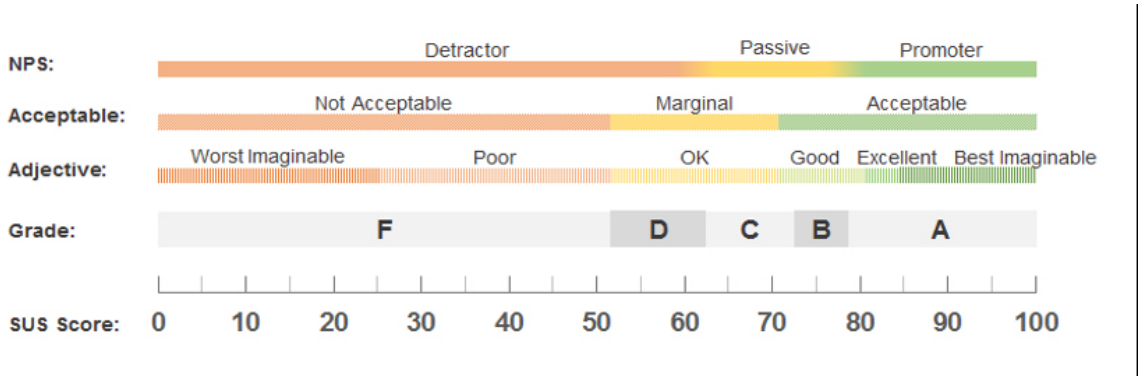


Fig. 2.7 Grades, Adjectives, Acceptability, and NPS Categories Associated with Raw SUS Scores.

End User Computing Satisfaction

End-User Computing Satisfaction (EUCS) is a metric that combines ease of use and information product items to assess the satisfaction of those who engage directly with a computer for a particular application. Ives, Olson and Baroudi (1983) define User Information Satisfaction (UIS) as one criterion for determining whether users believe the information system provided to them meets their information requirements [65]. The technique proposes a 18-item questionnaire that assesses five dimensions of end-user satisfaction "content, format, timeline and accuracy, along with easy to use"; as described in figure 2.8

EUCS, as defined by Doll and Torkzadeh (1988), is an individual's effective attitude toward a particular computer program based on direct interaction with the application. Satisfaction with end users can be quantified in terms of both primary (application) and secondary

user roles (inquiry and decision support application) [37]. The method is sufficiently reliable and valid across a range of applications. It is concise, easy to use and suitable for both practical and research purposes. Standards are made available to practitioners for their use. Similarly, its diverse components enable researchers to formulate and test more precise research questions [130].

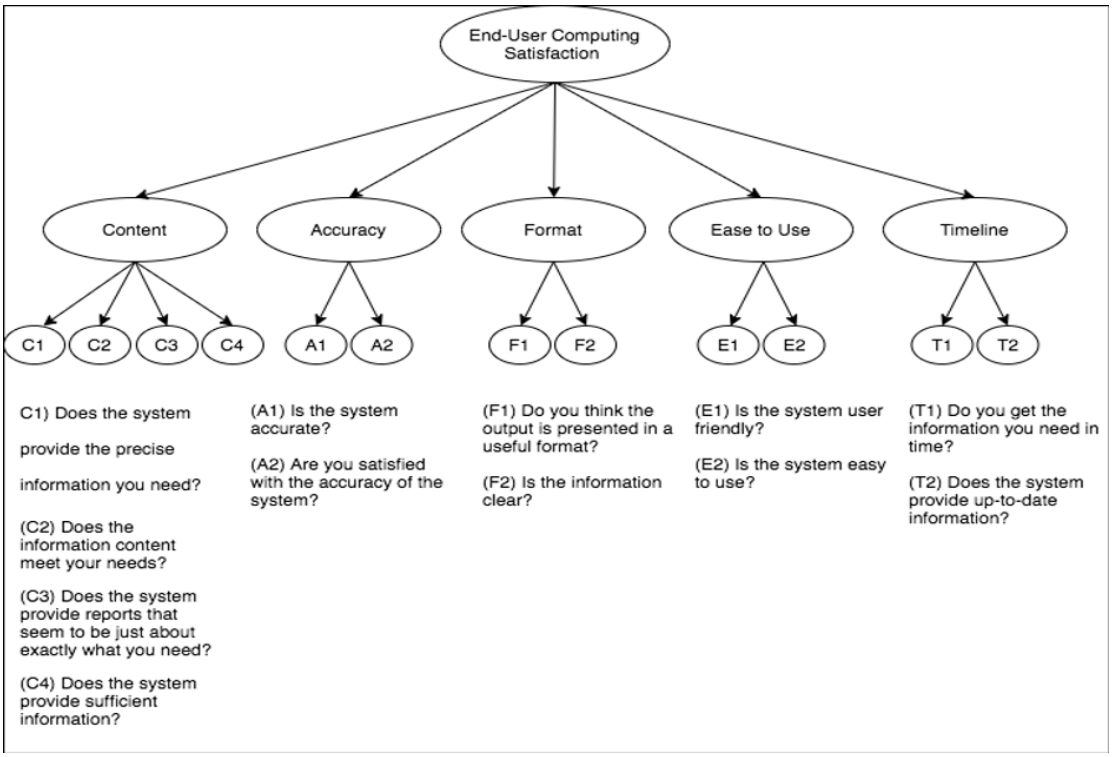


Fig. 2.8 End-User Computing Satisfaction Model.

Internal consistency, test-retest reliability, content validity, construct validity, and external validity have all been demonstrated to be adequate by EUCS [1]. This study analyses the data using descriptive analysis to constructively describe, show and summarize data points. We used Cronbach's Alpha test to validate the results of this test [91].

Questionnaires

Questionnaire is a research tool that consists of a series of questions that are used to gather data from respondents. The questionnaire method is one of the critical ways of data collection where researchers can measure specific variables or objectives through structured questions [136]. However, in any questionnaire study, the validity and reliability of the data collected must be ensured by researchers in order to analyse the data collected [100]. In general, there are three types of questionnaires:

1. Qualitative questionnaires, closed-ended or structured.
2. Quantitative questionnaire, open-ended or unstructured.
3. Mixed-method questionnaires, a mixture of closed-ended and open-ended.

However, each type of them has its pros and cons. For example, according to Seliger and Shohamy (1989) [60], quantitative or close-ended questionnaires are efficient and provide more accurate results that can easily be analysed. In contrast, Gillham (2000) [54] argues that open-ended questionnaires can result in a significant level of diversity and more difficulties in analysing results. In this matter, according to Alderson and Scott (1996) [3], the quantitative questionnaires are more accurate and reflect participants' opinions. Therefore, the mixed-methods questionnaires are the most appropriate data collection method for researchers.

Interview

The other type of data collection is the interview, where the researchers can gather information directly from participants. The interview is to reveal existing information so that it may be expressed as answers and therefore made interpretable Flick (2006) [45]. The interview can be person-to-person or group meeting, both of which are goal orientated conversation, as defined by Merriam (1998) [82].

2.7 Conclusion

This chapter provides a background to the topics related to the research conducted out within this thesis, including introducing background information of the research undertaken in blockchain-based solutions to facilitate the issuance of digital certificates and exploring their features. The topics covered in this chapter include an overview of blockchain-based applications structures and an overview of blockchain technology. Additionally, this chapter provides an introduction to smart contracts and their structures. Furthermore, blockchain platforms are covered in this chapter with a further explanation of Ethereum blockchain. This chapter also provides an overview of hashing algorithms. Moreover, it provides details of the system usability scale (SUS) test and the End-User Computing Satisfaction (EUCS) test. The research methodology was presented in detail in this chapter. In the next chapter, we conduct a systematic mapping study of the blockchain-based applications in Higher Education and study their structures, aims and limitations. The motivation behind this is to identify the issues relevant to utilising blockchain technology in such solutions.

Chapter 3

Blockchain-Based Applications in Higher Education: A Systematic Mapping Study

Overview

This chapter presents a systematic mapping study to collect and analyse relevant research on blockchain technology related to higher education. The chapter concentrates on two main themes. First, it examines state of the art blockchain-based applications that have been developed for educational purposes. Second, it summarises the challenges and research gaps that need to be addressed in future studies. The result shows six categories of blockchain applications in the higher education field and eight different challenges the use of blockchain applications in higher education could prevent.

3.1 Method

The main research questions behind this study were: " What are the research topics on blockchains for higher education?" and "What are the research challenges for blockchains in relation to higher education?" A systematic mapping design was used, following guidelines from [95] to explore blockchain applications related to education (see Fig. 3.1). Systematic mapping studies are similar to systematic reviews, except they employ broader inclusion criteria and are intended to map out topics rather than synthesize study results. A systematic mapping study provides a categorical structure for classifying the published research reports and results. The results of this study helped researchers to identify the gaps and challenges that need to be addressed in future studies.

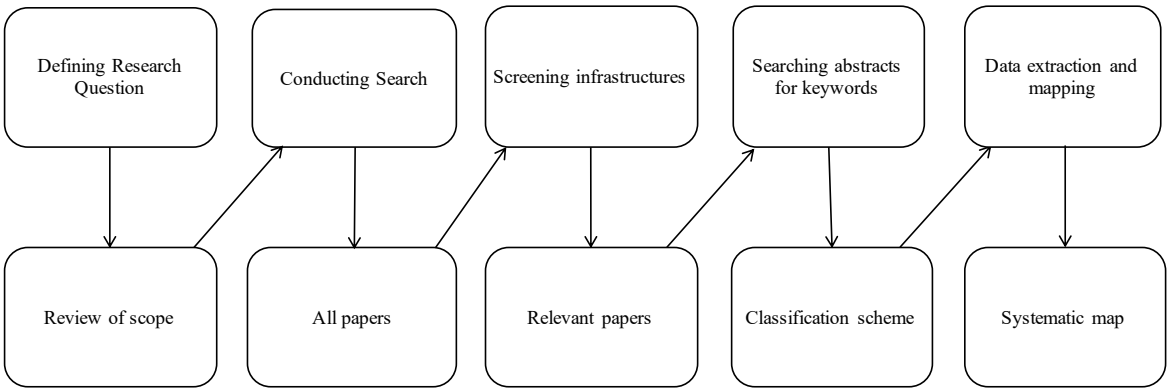


Fig. 3.1 Systematic Mapping Method Steps

3.1.1 Definition of Research Questions

In this step, we identified the research questions that our study aims to answer. For our study, we defined the following research questions:

RQ1: What are the research topics on blockchains for higher education?

RQ2: What are the research challenges for blockchains in relation to higher education?

3.1.2 Conducting Search

In this step, a search conducted for papers relevant to the research topic: blockchain applications in education. To narrow the focus of our study, the terms 'blockchain' and 'education' were selected as the keywords. Furthermore, well-known scientific databases were used to conduct the search: IEEE Xplore [40], ACM Digital Library [17], Springer [34] and Scopus. These selected scientific databases index high impact, high quality papers in the fields of education and information technology. Table 3.1 presents the query strings used to search each database. The focus was only on papers that had been published in conference proceedings, journals, workshops, symposiums and books.

3.1.3 Searching Abstracts for Keywords

In this step, all the relevant papers were classified by using the keyword technique explained in [129]. The main keywords were identified and the contribution of each paper from its abstract.

Table 3.1 Search Queries

Scientific Database	**Query Strings**
ACM digital library	[All: blockchain] AND] [All: higher] AND [All: education] AND [All: university] AND [Publication Date: (01/01/2017 TO 01/31/2020)]
IEEE Xplore	((((“Document Title”:blockchain) AND “Document Title”:higher) AND “Document Title”:education) OR “Document Title”:university)
Springer	‘blockchain AND higher AND education AND OR AND university’
Scopus	TITLE-ABS- KEY (blockchain) AND TITLE-ABS- KEY (higher education) OR TITLE-ABS- KEY (university) AND (LIMIT- TO (PUBYEAR , 2020) OR LIMIT- TO (PUBYEAR , 2019) OR LIMIT- TO (PUBYEAR , 2018) OR LIMIT- TO (PUBYEAR , 2017))

3.1.4 Data Extraction and Mapping

This process was conducted to collect the required information to address the research questions of this study. Therefore, The review criteria was designed to contain nine elements to review the papers, as shown in Table 3.2. The review criteria were piloted on a sample of five papers and then applied to the rest of the papers to extract data.

Table 3.2 Criteria for reviewing papers

Criteria	**Description**
Title	Title of the paper
Author(s)	Author's name(s)
Paper type	Conference, workshop, journal or book chapter
Paper topic	The topic area and subject
Publication date	Publication year
Publication location	conference country or organisation
Paper purpose	Aim of the paper
Application Implementation	System structure and implementation
Challenges	Actual and potential challenges

3.2 Study Results

We obtained a total of 108 articles. In the first stage of the screening process, we removed 47 irrelevant articles based on our criteria. Articles were omitted for two reasons. For the reason that we were concentrating on research of blockchains from a technical standpoint in higher education, we omitted papers that were not about higher education specifically. We also omitted papers that discussed the general aspects of a blockchain. Subsequently, 19 additional papers were discarded as duplicates, resulting in 42 papers. Thus, we analysed 42 papers for our systematic mapping research.

Figure 3.2 shows the distribution of papers by the year of publication. It is important to note that all of the papers were published after 2016. This indicates that this is a modern and novel area of research. Thus, the number of publications on this topic appears to be increasing each year, reflecting an increase in interest in the adoption of blockchain in higher education.

The geographical distribution of primary papers is shown in Figure 3.3. This geographical distribution, which is spread across 18 countries, illustrates that the adoption of blockchains in higher education has received international research attention. The greatest number of articles (n = 10, 22.2%) were written by colleges or corporations in the United States. Spain

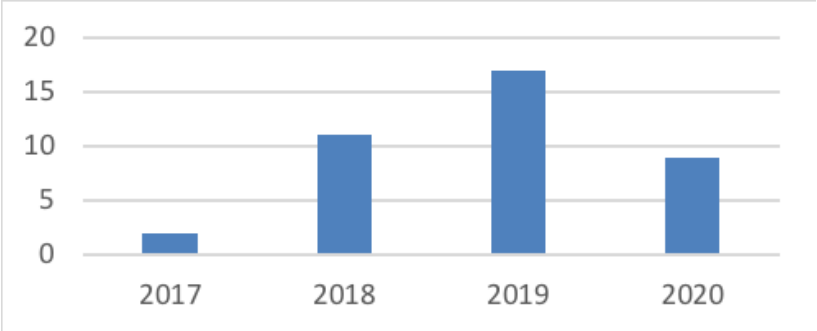


Fig. 3.2 Number of papers per year

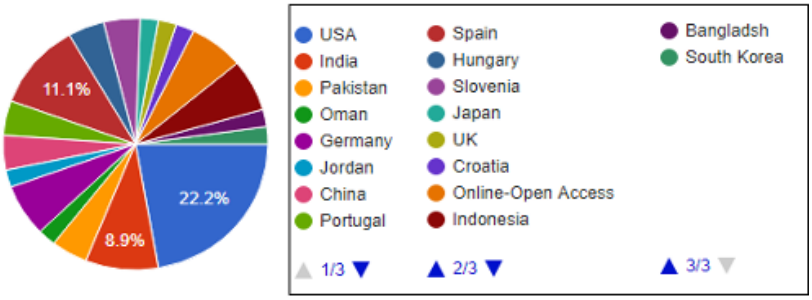


Fig. 3.3 Geographical distribution of primary papers

procured second place with four papers (11.1%). while three papers were published in India. The remaining papers were published in other countries.

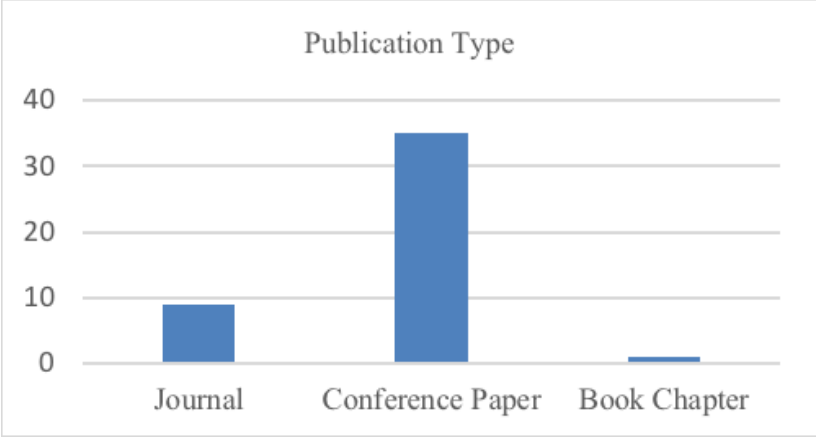


Fig. 3.4 Distribution of publications by type

Fig 3.4 presents the distribution of publications by type. The vast majority (37 papers) of these articles were published in conference proceedings, whilst were published in journals and one published as a book chapter. The Institute of Electrical and Electronics Engineering

(IEEE) had the most publications. Approximately 65.63% of the venues were technical venues, while 34.38% were educational venues.

Table 3.3 shows the classification categories relating to the papers. In this step, we classified all the relevant papers by using the keywording technique explained in [12]. We identified the main keywords and classified each paper from its abstract.

Table 3.3 Classification categories

Criteria	**Papers**
Certificate/degree verification	[9][24][43][56][57][67][70][77][78][79][99][114]
Student assessments & exams	[33][84][109]
Credit transfer	[111][116]
Data management	[21][44][46][73][79][81][92][93][98][108][132][133][135]
Admissions	[48][87]
Review papers	[2][9][21][30][44][68][74][104][117][129]

Description of the Categories

Certificate/degree verification: This category included studies of blockchain technology that can assist with validating student diplomas and can provide greater control over how students earn certificates.

Students assessments & exams: Articles in this category described automated mechanisms for the production of exams and assessment schemes for university students.

Credit transfer: This category included research on blockchain applications for storing student records and transcripts and transferring academic credits between universities.

Data management: This category contained articles on blockchain applications to assist with connecting students' records across institutions as well as smart contracts to manage student data and storing their records.

Admissions: These articles proposed blockchain applications to facilitate students when applying to universities by storing and sharing the admission procedures and required documents to apply to a particular university.

Review papers: These included literature review studies conducted by researchers during the period defined in this study.

3.2.1 Articles by Classification Categories

Table 3.4 presents the distribution of publications by the challenges detected when reviewing the scientific literature included in the search results.

Table 3.4 Classification of challenges

	Category				
Challenge	Certificate "degree verification"	Assessments & exams	Credit transfer	Data management	Admissions
Privacy	[9][57] [114]	[109]	[116]	[21][46] [79][92]	[49][87]
Immutability	[117]	[84]			[48]
Blockchain usability	[57][67] [77]	[84]	[111]	[92][135]	
Cost	[76][78]	[84]		[98]	
Scalability	[67]		[116]	[46][81] [98]	
Consensus algorithms	[67][76] [78]	[109]			
Blockchain platforms	[87]			[21]	
Motivation	[76][78]				[48]

As shown in Figure 3.5, the majority of studies on blockchain applications in higher education focused on the management of certificates. Of the 42 publications analysed, 12 (28.57%) focused on the verification of degrees. Three papers (7.14%) examined blockchain applications concerning student assessments and exams. The third type of application focused on the transfer of credits and included two articles (4.76%). The fourth application type concerned data management and comprised four articles (30.95%). Two of the papers (4.76%) focused on blockchain frameworks to ensure security and protection in the admission systems. Finally, the sixth type was review papers that examined potential methods of implementing blockchains in higher education.

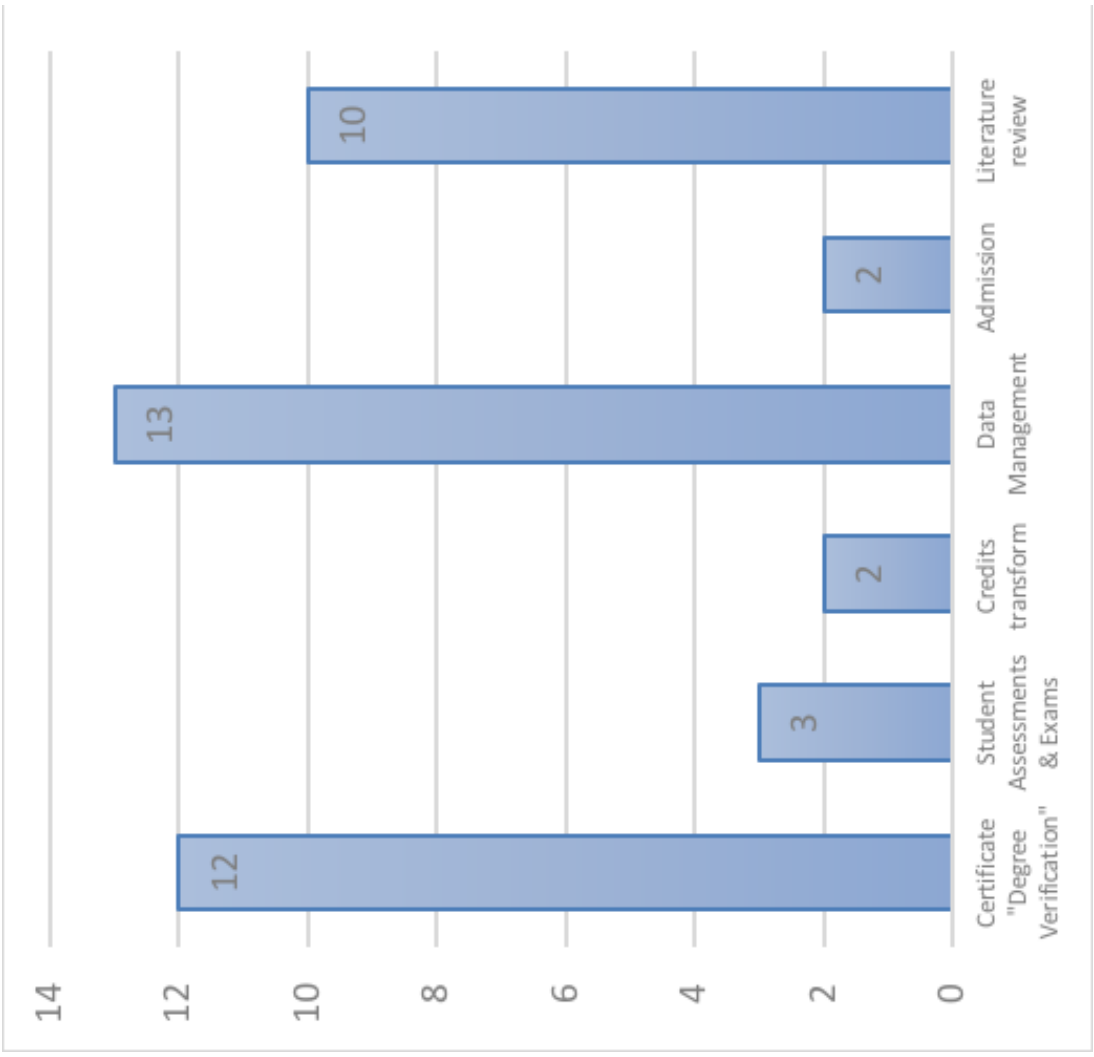


Fig. 3.5 Articles by Classification Categories

3.2.2 Classification of challenges

Figure 3.6 illustrates the nine challenges presented in the reviewed papers. The first challenge, consisting of 11 articles, concerned blockchain privacy. These articles examined different privacy concerns that may arise with regard to blockchain technology. Furthermore, immutability (with three articles), a major aspect of blockchains, may become a problem when implementing blockchain technology in higher education. Immutability can make it complicated for educational institutions to enforce new laws on data storage or correct inaccurate data. The third challenge involved the complicated nature of blockchain technology, as stated in seven articles. For example, certification authentication can become a challenge when using blockchain technology in education [84]. The cost of using blockchain technology was the fourth challenge and comprised four articles. Five articles observed the issue of blockchain scalability. As the number of blockchain blocks increases, so does the processing time, which can have an impact on the performance. Articles two and four focused on consensus algorithms and blockchain platforms, respectively, and noted that educational institutions may face challenges when identifying which data and services need to be introduced in the blockchain network. The final challenge concerned the reasons for using blockchain technology, with three articles noting that immaturity problems, including complicated settings and low usability, have a sustained impact on blockchain's implementation in higher education.

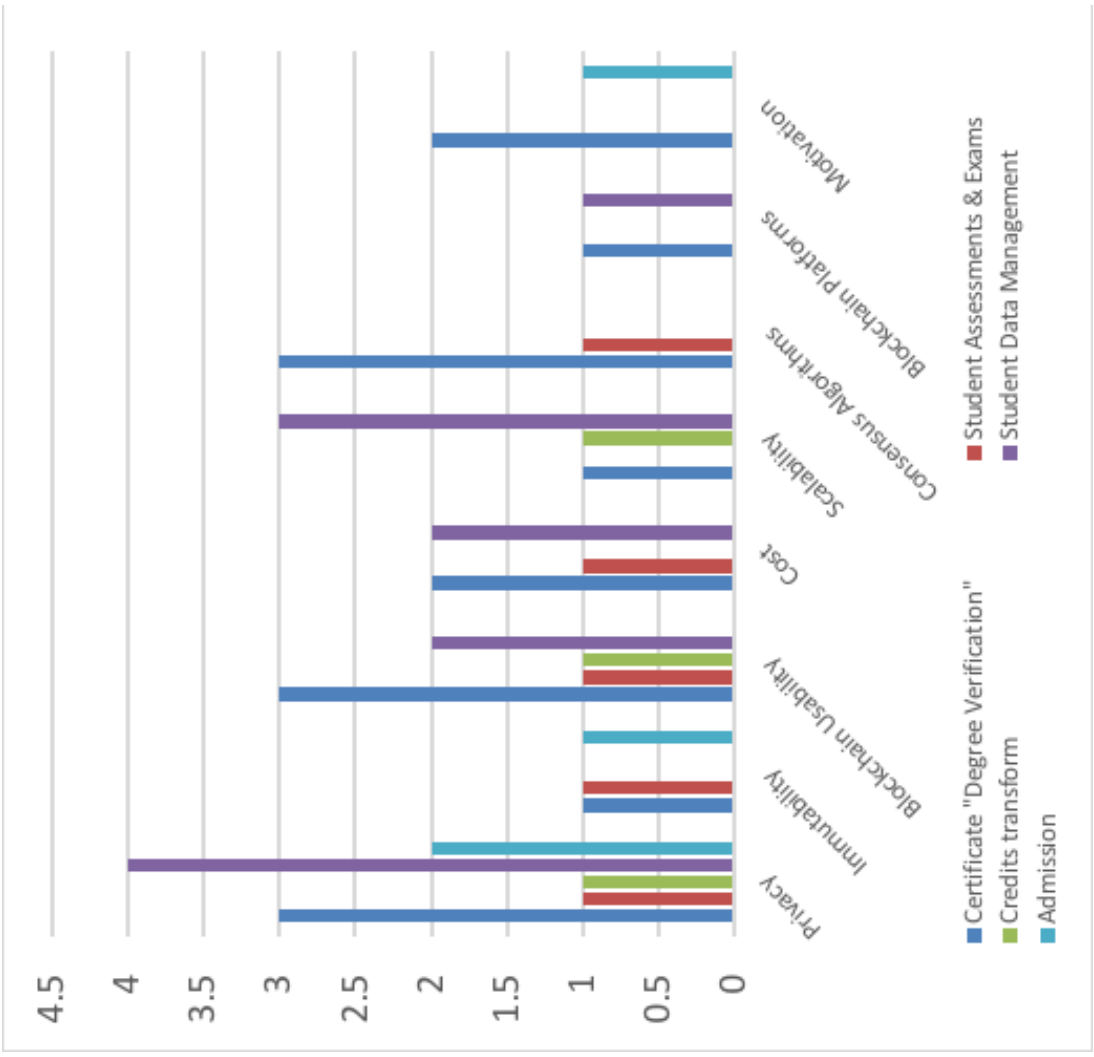


Fig. 3.6 Classification of Challenges

3.3 Discussion

According to the publication trend, the utilisation of blockchain innovation for higher education has been met with increasing enthusiasm. As there have been relatively few studies related to this subject, there is a need for further research examining the potential use of blockchains for education. The evaluation of the 42 studies presented here can help in addressing two major research questions.

3.3.1 First Research Question

This study was inducted as a part of this thesis to provide an answer to the **Question 1** identified in chapter 1, in particular, the first sub-question listed under the main one. Which is: What are the current blockchain applications in higher education? What are their features and limitations?

This study designed to answer the following research questions:

RQ1: What are the research topics on blockchains for higher education?

What are the current blockchain applications in higher education? What are their features and limitations?

Although there have been numerous blockchain-based applications developed for educational purposes, few have been utilised by stakeholders. Such applications can be classified into six categories, as presented in Table 3.3.

Certificate/degree verification

The first category focused on specific applications intended to confirm certificates and verify degrees. This category included all research addressing academic certificates and transcripts for higher education students. Verification of academic certificates is crucial for employers as well as other authorities to confirm the authenticity of an academic degree. Following up with and verifying the status and authenticity of a diploma is problematic and blockchain technology presents a promising solution [117]. The applications in this category tended to focus on authorising universities to provide students with access to official certificates and ensuring information privacy.

Han et al. [57], for example, introduced a unique blockchain-based method for universities to authenticate and share official education certificates. Budhiraja and Rani [24] also presented the TUDocChain platform, which enables academic certificates to be reliably and sustainably

authorised on a public ledger as a practical solution in relation to issuing, validating and sharing certificates.

Student assessments & exams

The second category focused on student assessments and exams. These studies intended to fulfil the quality standards as well as requirements established in the relevant programmes and curricula. Mitchell et al. [84] introduced dAppER, an automated quality assurance mechanism that uses established internal procedures to develop exam papers and their related evaluation schemes.
This technology offers a robotised quality affirmation system to develop test papers and their appraisal plans, wherein a permissioned blockchain protects the tests and sustains the audits' immutable and trusted ledger. Shen and Xiao [109] proposed a model that uses blockchain technology to verify students' answers.

Credit transfer

The third category involved applications for transferring students' credits between universities. These applications are intended to enable a university to transfer completed course credits to another university. In this category, applications were presented to transfer credential records between colleges, establishments or associations, given blockchain's high security and trust. Srivastava et al. [111] proposed a framework to store student records and transcripts that included an electronic credit transfer mechanism. Hence, students are able to transfer completed course credits between different universities. Turkanović et al. [116] also proposed a global higher education credit platform called EduCTX, which follows the European Credit Transfer and Accumulation System.

Data management

The fourth category involved data management applications that can gather, report and assess university data to automate rules, support decision making and protect students' identities and their data. Bore et al. [21] examined the initial structure, implementation and assessment of the blockchain-enabled School Information Hub by conducting a case study of Kenya's school system. In addition, Filvà et al. [44] presented a blockchain-based solution for automating rules and constraints so that students can control their data and ensure their privacy and security. Forment et al. [46], also proposed various actions intended to safeguard students' identities and to secure their data by means of new technologies, including blockchain.

Admissions

The fifth category concerned blockchain applications connected to university admissions and student registration. Mori and Miwa [87], for example, presented a digital university admission application system that organises study documents and e-portfolios through smart contracts on a blockchain. Curmi and Inguanez [33] also proposed a platform that registers students and includes their medical records while ensuring that their sensitive data remain private, with the information owner in control of access to these documents. Moreover, Ghaffar and Hussain [48], introduced the blockchain-embedded academic paradigm to augment legacy education through an application (CEAP), enabling students to apply for university admissions via a single platform.

Review papers

The final category involved literature reviews of studies focusing on higher education and blockchain applications. Overall, eight papers examined this topic. In the literature reviews, preliminary investigations and evaluations were student centred and focused on recordkeeping and sharing using a trusted and safe platform, such as in [2][30][70][117][129].

3.3.2 Second Research Question

RQ2: What are the research challenges for blockchains in relation to higher education?

Although blockchains have several beneficial applications for education, researchers continue to face numerous problems in utilising this technology for education. Hence, several challenges were detected in the reviewed papers.

Immutability

The term 'immutable' came up repeatedly in relation to blockchains. Blockchain's immutability results in it becoming impossible for the data stored in the blocks to be changed, which is a crucial aspect of blockchain technology. However, immutability is a significant challenge to using blockchain technology for education, such as diploma revocation. Although this is not common, it can be used when there are unique circumstances in which diplomas are withdrawn. The diplomas that are stored on the blockchain, however, cannot be changed because of blockchain immutability [117]. Hence, immutability can decrease blockchain's applicability in terms of students' sensitive data. This challenge applies specifi-

cally to three categories in which students' information needs to be stored on the blockchain: certificate/degree verification, exams/assessments and admissions.

Blockchain Usability

Blockchain technology's usability is also a major challenge in the field of education. The technology's terminology is often ambiguous, and it is perceived as lacking maturity. Moreover, the user may have to deal with several complicated settings to ensure security, such as primary keys, recovery roots and public keys. It should also be noted that a P2P network blockchain includes very different specifications compared to those intended for individuals, which can make using blockchains difficult for end users. Thus, blockchain usability should be enhanced by application design interfaces, which allow individuals who do not have technical expertise to use blockchain more easily [99]. Thus, further studies on blockchain usability for individuals are necessary. In addition, blockchain adaptation can be improved in the education field through well-designed interfaces with simple specifications.

Privacy

It is important to consider how data can be securely accessed and used while maintaining privacy [57]. Blockchain systems use private and public keys to protect user identities. Public keys are publicly visible, indicating that the blockchain cannot guarantee transactional privacy. Thus, blockchain privacy protection mechanisms have drawbacks that may lead to anonymous abuse. Hence, it is crucial to protect the identities of students by creating a mapping connection between the students' pseudonyms and real identities [109].

Cost

A further challenge concerns the cost involved in blockchain transactions, as managing and storing substantial amounts of student data on the blockchain can increase mining costs. Hence, it is necessary to manage development and operational costs of using blockchains in traditional education systems [78].

Scalability

Scalability concerns how the ever-increasing number of participants and assets as well as larger transaction sizes can impact the blockchain applications' access latency. When addressing large sets of data and metadata, particularly regarding education, scalability should be dealt with in the preliminary architecture. It is difficult to foresee the direction and extent

of blockchain technology considering potential future adaptations and new implementations for scalability [46].

Blockchain platforms

It is thus necessary to determine whether it is better to store the data on the blockchain or encrypt it and store the decryption keys on the blockchain. Existing blockchain platforms, including Bitcoin and Ethereum, are able to process approximately 10–15 transactions per second on average. Centralised applications used by credit card companies such as Visa can process approximately 5,000 to 8,000 transactions per second on average. Furthermore, as miners are more inclined towards high gas transactions (the highest-price-first-served model), transactions costs can increase.

Consensus algorithms

As sensitive education information is stored in the blockchain, developing a secure blockchain system is a vital research area. Several researchers have focused on developing consensus algorithms for safeguarding transaction data. Using blockchain technology in the field of education may also include the development of consensus algorithms with the most benefit [78][109].

Motivation

Another challenge is a lack of motivation. It is difficult to encourage stakeholders to implement blockchain-based applications in the traditional systems of education that have now been in place for a considerable time. Thus, further studies on blockchain usability for individuals are essential. Blockchain adoption can be improved in the education field by way of the development of usable blockchain-applications [48][76][78].

3.4 Summary

Blockchain is a distributed ledger technology that utilises cryptography techniques and distributed consensus algorithms for decentralisation, immutability and traceability. The properties offered by blockchain and smart contracts can lead to several innovative applications in the context of higher education. It is possible to use blockchain technology for education in various innovative ways besides managing diplomas and evaluating achievements. This systematic mapping review study aims to address this issue by illuminating existing blockchain applications for higher education and highlighting the research challenges

associated with implementing blockchain technology. The main purpose of this study is to answer the research questions **"What are the current blockchain applications in higher education? What are their features and limitations?" in Chapter 1, page 5**. The study results can help future research to identify and resolve additional challenges. The most important insights we gained from this study are identifying the taxonomy of the blockchain applications in higher education that contains six different areas and also identifying the eight principal challenges that applications include. In the subsequent chapter, we conducted a study to investigate the requirements of building a Blockchain-Based Trusted Achievement Record System for students in higher education.

Chapter 4

Investigating the Requirements for Building a Blockchain-Based Achievement Record System

Overview

This chapter presents important information on the thoughts and outlooks of stakeholders on an achievement record system that uses blockchain and smart contract technology. The system would allow stakeholders (for example employers) to validate learning records. Two main things are investigated. The first is to evaluate the suitability of the idea of building a trusted achievement record for learners in higher education and to evaluate potential user knowledge of blockchain technology. This is to ensure that a designed system is usable. The second aim includes an interview conducted with a small group of participants to gather information about the challenges individuals have when creating and reviewing CVs.

Overall, 90% of 247 participants agreed that there was a strong need for a trusted achievement record. In addition, 93.64% of respondents stated that they felt it was invaluable to have a system that is usable by all stakeholders. When tackling the second aim it was found that a primary challenge is lack of knowledge of blockchain and its complexity. From the employers' perspective, there is a lack of trust due to inaccuracies when students describe skills and qualifications in their CVs. In Section 4.5, we present the results of the two studies conducted in this chapter. Section 4.5.1 presents a detailed analysis of the questionnaire findings. The second study involved interviews with six participants responding to a questionnaire to address certain open-ended questions, Section 4.5.2 presents a detailed analysis of the findings of the interviews. Section 4.6 presents a discussion of the two

studies results, whilst Section 4.7 presents the recommendations. Finally, the conclusion is in section 4.8.

4.1 Contribution

The main contribution of this chapter is to gather useful information from participants about their thoughts concerning developing a blockchain-based achievement record system using smart contract technology in order to determine the requirements for the conceptual design of the Blockchain-Based Trusted Achievement Record System.

4.2 Objectives

This study aims to collect valuable data from participants that reflect their opinions and thinking regarding the building of an achievement record system based on blockchain and smart contract technology [28]. Once the data has been gathered, the system requirements can be established, as well as the necessary tools and mechanisms involved. This aim can be fulfilled with a number of objectives:

1. To develop user friendly and reliable records for the stakeholders, such as students, employers and academic staff.
2. To gather essential information from participants of varying educational levels and job roles.
3. To offer analytical information on stakeholder outlooks on holding a validated achievement record.
4. To establish the difficulties and disparities of achievement record validation.
5. To offer analytical information about the average time necessary for the validation of achievement records.
6. To present stakeholders with reliable, detailed CVs with all the information they need.
7. To offer enough analytical capability to stakeholders in order for them to possess their necessary information.
8. To provide analytical information with which achievement records can be developed reliably.

9. To pinpoint the data users requirements in order to show their achievement record.
10. To pinpoint the data users require in order to show their achievement record.
11. To establish how much comprehension of blockchain and smart contract technologies people possess, in order to tailor the user experience (UX) design of the system.
12. To find how difficult the user interface (UI) is to use, in order to tailor a prototype UI.

4.3 Method

This study uses a mixed-methods approach [96]. It involves the collection of data quantitatively using a questionnaire using a closed set of questions [97]. The questionnaire is created in such a way that numerical data is efficiently collected for further analysis later to produce a generalizable result. The mixed-methods approach also involves a qualitative approach through interviews with a number of participants comprised open questions [53]. The first study was a questionnaire distributed to approximately 1000 people of varying educational levels and job roles [32]. A response rate of 24.7% (n=247) was achieved and basic descriptive statistics and specific cross-tabulations were used to analyse the findings. 'SurveyMonkey' [120] was used to design the questionnaire.

4.3.1 Participants

We aimed to reach the maximum number of participants to respond to the questionnaire in 30 days. The target participants were people in different occupations and academic levels. We used various methods to invite respondents, such as email, social media applications and SMS messages.

4.4 Reliability Test

As a result of the statistical data, the reliability of the variables intends to measure the overall consistency under different conditions. Thus, the value of Cronbach's Alpha needs to consider how the internal consistency can be measured. Typically, the standard value to measure reliability is greater than 0.5 [91]. This indicates the variables' accepted level.

Data Interpretation:
In the current case, Cronbach's Alpha value is 0.638 as shown in Table 4.1, indicating strong reliability since the value is greater than 0.5. It can also be said that the estimated value greater than 0.638 indicates the best reliability, reflecting the strong interrelation between all variables.

Table 4.1 Reliability Statistics Investigation Study.

Cronbach's Alpha	N of Items
0.638	17

4.5 Results

4.5.1 Study 1: Questionnaire

The first step was to set a question which was able to evaluate the education level of the participants. Figure 4.1 shows that the education level is divided into eight categories, ranging from 'Less than a high school degree' to a 'PhD or other.' The results show that the respondents had a range of educational levels, meaning that the data received is richer as a result of the participants coming from a variety of educational backgrounds. Regarding the sample in the current study, 38.87% hold a bachelors, 35.22% a masters (35.22%) and 14.17% a PhD.

Next, the occupations of the study sample collected are shown in Figure 4.2. Most of the participants were academic staff (53.043%), whilst students comprised (8.10%). It is significant that each person involved would be the beneficiary of the proposed trusted achievement record.

Validating the information provided in the CV is an essential process for stakeholders (for example, employers, administrative staff). In the scope of the current study, the method of verifying data in CVs was investigated. Within the questionnaire, participants were asked the question: "What do you do to check the validity of data in the CV?" 136 of the participants'

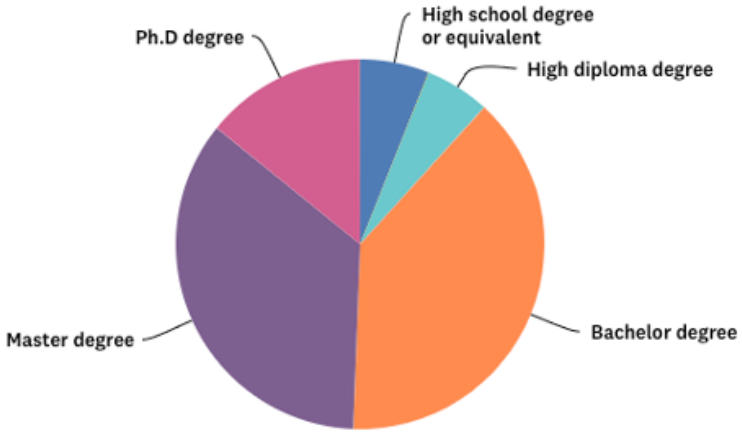


Fig. 4.1 The respondent's education level

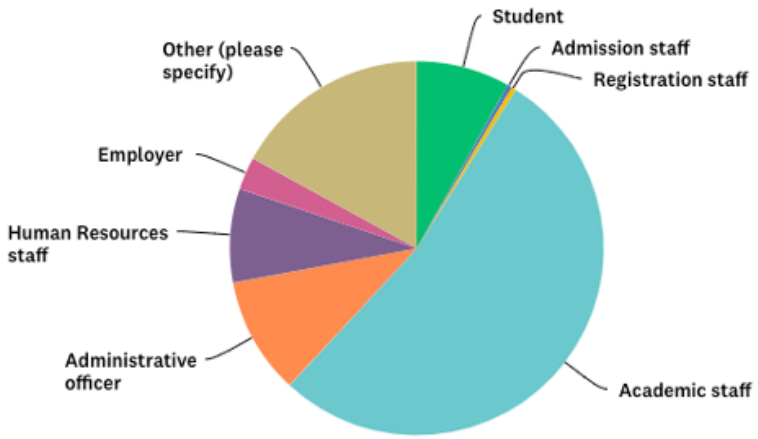


Fig. 4.2 Participants' occupations

answers were received. In Figure 4.3, it can be seen that 81.62% require the original copy of a certificate from the applicants, while 25.74% contact the issuer of the certificates by email, phone, etc. Additionally, 16.91% require the original copy in a closed and sealed envelope from the issuer and 5.88% take advantage of other methods like digital signatures.

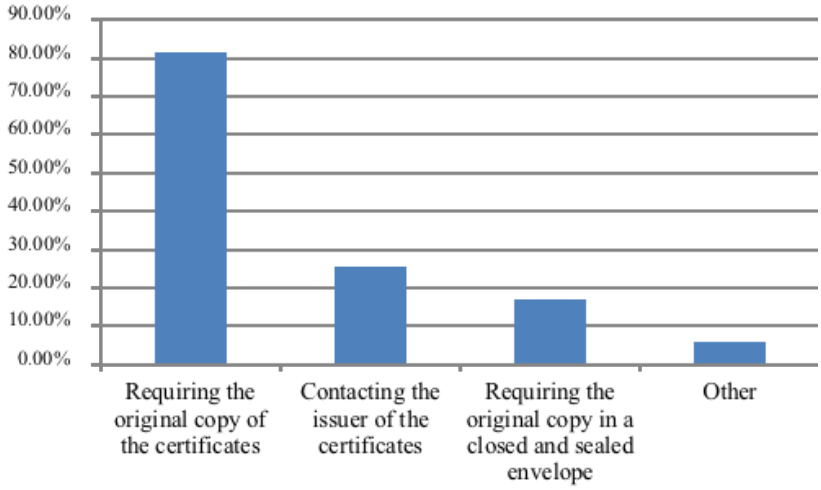


Fig. 4.3 The methods used to verify data in CVs

We also examined the time it takes to validate the correctness of information presented within CVs. Asking the question: "How long does the validation process take?". Figure 4.4 illustrates the distribution of responses from 136 participants. As the figure shows, on average, record validation takes 12 days.

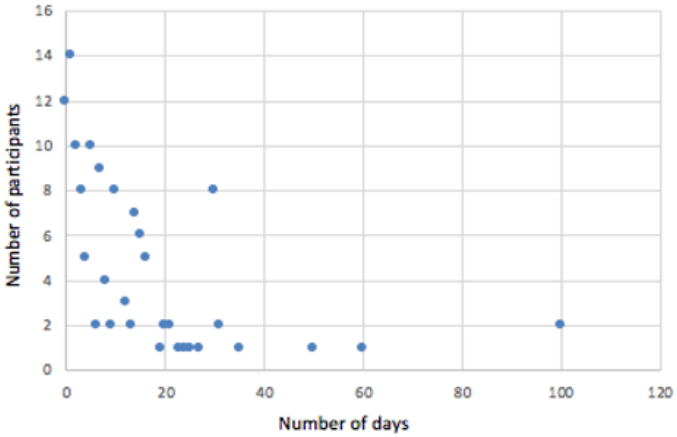


Fig. 4.4 Time participants take to validate CVs data

Next, the participants were asked what the key content of their trusted achievement record would be. Their answers were able to confirm that the core components of trusted records

would be education certificates, recommendation letters, standardised tests, language ability, training completed, achievement certification and certificates earned, as shown in 4.5.

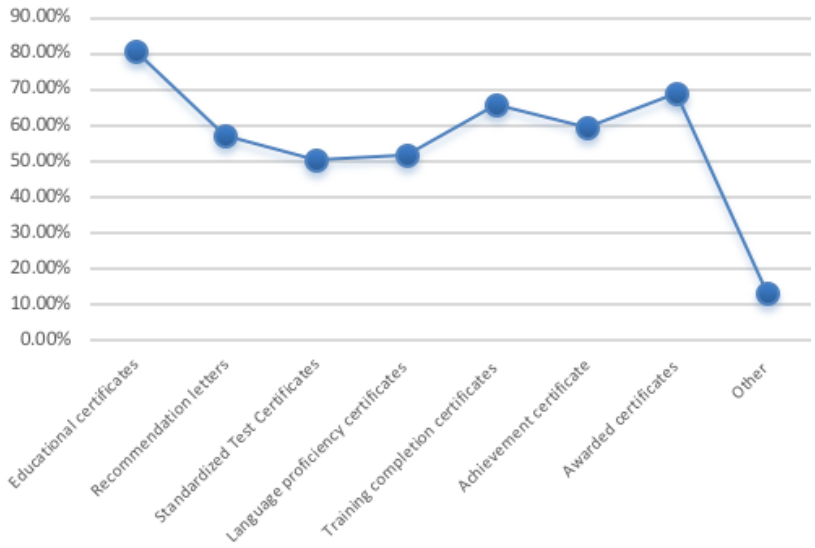


Fig. 4.5 contents selected to be added to the Achievement Record

The participants were then asked to state if they felt that the trusted achieved record is beneficial. It was shown that 64.74% strongly agreed with this notion. A total of 93.64% either agreed or strongly agreed. Their responses can be seen in Figure 4.6.

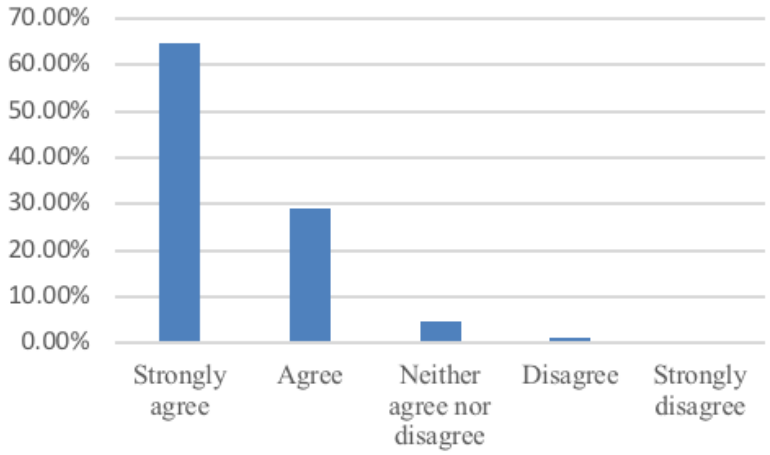


Fig. 4.6 Trusted achievement record usefulness

In Figure 4.7, it can be noted that the majority of respondents (55.32%) did not have any understanding of blockchain technology, while 80% of participants also said that they have never undertaken a transaction using blockchain technology.

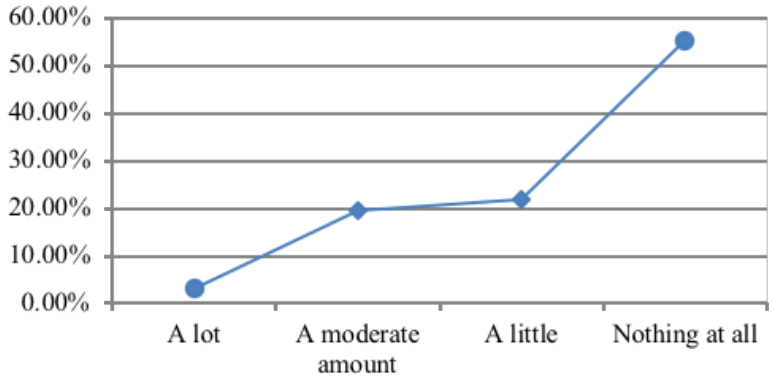


Fig. 4.7 Participants' knowledge of blockchain technology

The participants were then asked about their awareness of digital wallets. As shown in Figure 4.8, (44.15%) had no knowledge of digital wallets and most stakeholders (71.70%) had never used digital wallets, Ethereum wallets or MetaMask. Conversely, (28.30%) of participants had experience of dealing with digital wallets [15].

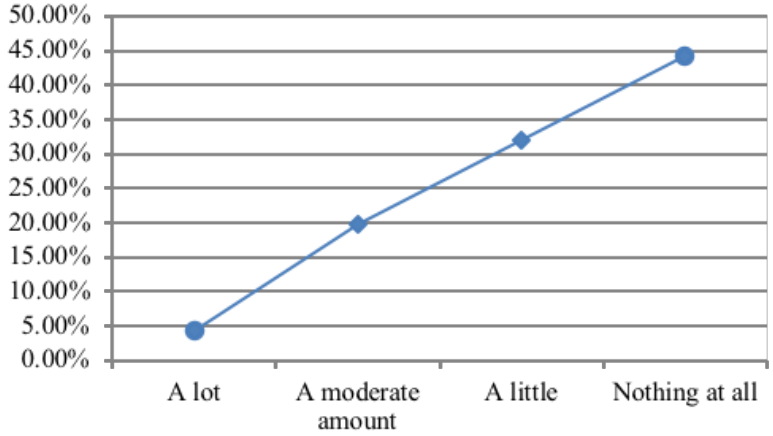


Fig. 4.8 Participants' knowledge of digital wallets

4.5.2 Study 2: Interview

Interviews were undertaken with six participants, with the intention of gathering data about the problems they had when developing their CVs or when attempting to use them. Table 4.2 describes the individuals taking part in the interviews.

Table 4.2 Participants Interviewed

Participant	Occupation
P1	Student
P2	Registration staff
P3	Admission staff
P4	Academic staff
P5	Human Resources
P6	Employer

Two direct questions were asked, which were: what is the challenge they face when creating their CV? And what are the problems they encounter when reading or reviewing other CVs?

Validation of the interview design

To validate the interview questions, the inter-rater reliability method [8] was applied. We investigated the validity of the interview design through *a design critique workshop* for multiple reasons. First, it yields valuable feedback quickly and regularly. Second, it allows people to provide direct constructive feedback on the design. Third, it builds resilience in the designer to be open to criticism of their work and thus improve its quality. To achieve our aim, we designed the workshop using the "Six P's" [47] framework (See Table 4.3) to manage the quality of the process [131].

Table 4.3 Six P's workshop framework.

Purpose	Participants	Principles	Products	Place	Process
Why do we do this workshop?	Who is involved?	How do we function?	What do we do?	Where is it located?	When is the meeting?
To validate the interview	experts.	Meet the group and discuss the interview questions.	Discussion.	School of Computing, Newcastle University, Meeting Room.	15/10/2020 From 10:00 am To 11:00 am

The process is efficient since we need a few numbers of experts. We met with two experts from the OpenLab group, School of Computing, Newcastle University, UK. The result of the discussion is that the experts agreed that the interview questions were suitable and direct, and valid to be used in the study.

4.5.3 Result

P1 stated that they are often confused about the structure of their CV and that while they can find many templates online, they do not know which would be the most appropriate choice. Further issues they had related to the amount of time required to complete their CV and the fact it needed frequent updates. Concerning the second question, they replied that they did not know. Their responses made it clear that the structure of their CV is an area of primary importance to the participant.

P2 respond differently. With respect to the first question they stated that they did not find anything difficult and that it is easy for them to organise their CV using a good structure. In relation to the second question, they believed that as an employee who handles registrations, they would firstly examine the personal information and address given, to make sure it is updated and that it matches their ID or passport information. This information will be placed in their system and then printed on the certificates. The main observation here is related to the lack of accuracy as regards users' information saved in the system and which will appear in their certificates.

P3, responding to question one, said that they can write their CV with no issue. For the second question, they felt that a CV is a necessary document when applying to university, and they have seen a great number of applicant CVs with mistakes, which meant that they requested the original documents. The observation of these answers is that there is a lack of accuracy in the provided documents in particulate the CVs.

In response to the first question, P4 said that they had no problem with CVs. Responding to the second question, they felt that people often over-described their current qualifications and skills. Thus, the initial observation for this question is that over-describing occurs based on the responses.

To the first question, P4 said that they had no issues. For the second question, they said that people occasionally emphasised skills on their CV for which they had no proof or certificates, meaning they had difficulty knowing if they were being honest. The observation in connection with this question is that trust issues exist regarding CV information as discussed in the introduction chapter.

Firstly P5 stated that writing a CV was easy for them, but that it requires time. This is especially the case for people who have numerous qualifications and abilities, as well as a long work history. To the second question, they said that while they review many CVs on a weekly basis, it is not easy for them to judge the individuals this way. As a result, they ask for an interview, a presentation or a practical test, in order to provide them with a better opportunity to evaluate the person. Similarly, contacting certificate issuers is a difficult process when seeking to verify certifications, hence they often delegate this task. Lastly,

every so often CVs include false information or the author has made clear mistakes. The initial observations for P5's answers are that there are issues associated with fairness, a need for more time and effort and issues concerning dishonesty.

For the first question, P6 revealed that creating a CV was not a complicated task for them. In response to the second question, they said that they take responsibility for choosing employees, as the success of the business depends on them. For the private sector, applicants skills are of greater value, so the interviews they conduct are primarily focused on skills. The problem they have is that they need to verify the qualifications on the CV. Likewise, applicants can over-describe their skills or even lie, as it is a competitive environment. The observation for this answer is that there are concerns regarding fairness, the extra effort needed, issues with dishonesty and the problem of over-describing.

4.6 Discussion

4.6.1 Study 1: Questionnaire

Of those who participated in the study, the majority of stakeholders check the validity of CV information prior to making decisions. An intuitive interpretation is that certain people have an immature and less developed approach toward their achievement records. As discussed earlier, CV fraud is pervasive and is predicted to increase even more in the future due to intense competition between job seekers [115]. This is reflected in our results, which demonstrate a lack of trust in the reliability of submitted CVs. When asking stakeholders how they prefer to verify information in CVs, their answers demonstrate a variety of methods as seen in Figure 4.3, notwithstanding that applying these validation methods may not be efficient and take time and effort. Improving the validation process efficiency in our opinion is an essential future research requirement, which we aim to address through the design and development of a trusted achievement record using blockchain technology [11].
Most respondents (91.71%) stated that they would like to have a trusted record of all their records of achievement. To determine the context of a trusted achievement record, we asked about essential information and documents that should be stored. The majority of respondents agreed that educational certificates are essential documents that should be stored. Moreover, participants answered that the record of achievement must contain other important documents (for example; awards, language proficiency docs, test results, etc.). Therefore, diversity of documents is a crucial factor to consider when developing such a system. We have demonstrated the level of knowledge among people concerning technology by way of an inductive and deductive set of questions. Consequently, most of the respondents

emphasised that they do not know much about blockchain technology. We asked participants who do have a background in blockchain if they had undertaken any transactions using blockchain. The feedback from most of the respondents reveals that they have no experience of performing a transaction using any digital wallet. Therefore, the ability to manage the complexity of blockchain technology is one of the primary challenges for researchers, whilst the lack of understanding and knowledge of the technology is a challenge for the end-users too. Thus, it is essential for future research to address these challenges while developing a blockchain-based system.

4.6.2 Study 2: Interview

We conducted interviews with selected participants to collect additional information concerning the issues and challenges they are facing in two situations. The first is when they write a CV and the other is when they read and evaluate candidate CVs in order to make recruitment decisions. Thus, we can identify gaps that need to be covered in future research. One of the problems is the diversity in the designs and structures of CVs. This diversity affects the quality of the CVs as well as efficiency of analysing and processing their content. Precision is another problem, especially when people describe their qualifications, responsibilities and jobs. Over-describing skills is a common occurrence, which is due to the increased competition between job applicants [89]. Consequently, trust in CV content, coupled with fairness when comparing CVs is affected and is a fundamental problem.

4.7 Recommendations

CV fraud is pervasive and has negative consequences; it damages organisations/employers, is unfair on qualified applicants with honest CVs and it can tarnish reputations, increase hiring and training costs to replace fraudsters who have had their employment terminated, propagate unethical cultures, cause poor performance when job-related skills are lacking or risk legal charges related to negligent hiring [92]. The results of the work described in previous sections demonstrates that the majority of the participants in our study agreed that it is necessary to develop a trusted achievement record capable of addressing the highlighted problems.

In this chapter we recommend exploration of the design of a blockchain-based system that provides a trusted achievement recording service with consideration to the needs of users, as discussed in section 4.6. Considering the lack of knowledge in blockchain and its use, as confirmed previously, handling blockchain technology's complex nature should be a key area

of attention for researchers. The poor comprehension of this technology is a major hurdle for end-users. Therefore, it is recommended to invest effort in the design of a friendly user interface to facilitate dealing with the complexity and usability of this promising technology.

4.8 Conclusion

Recording and verifying achievements using blockchain technology has plenty of potential and important advantages, including the potential to offer superior usability and efficiency compared to legacy systems. Our aim is that the findings of this work can serve as a platform to undertake future research towards eliminating credential fraud and to facilitate the creation of a trusted achievement record that can be easily shared and used by interested stakeholders in a usable and trusted manner. Furthermore, the outcome of this study provides essential information to design a blockchain-based trusted achievement system. This study was conducted to answer the research questions:**"How to determine the requirements for building a blockchain-based achievement record system?" in Chapter 1, page 5**. In the next chapter, we propose a conceptual model of the Blockchain-Based Trusted Achievement Record System based on the outcomes of this chapter.

Chapter 5

Blockchain-Based Trusted Achievement Record System Design

Overview

The primary purpose of this chapter is to provide a design for a blockchain-based system, which produces a verifiable record of achievements. Such a system has a comprehensive range of potential benefits for students, employers and higher education institutions. A verifiable record of achievements should enable students to present academic accomplishments to employers, within a trusted framework. Furthermore, the availability of such a record system would enable students to review their learning throughout their career, giving them a platform on which to plan for their future accomplishments, both individually and with support from other parties (for example, academic advisors, supervisors or potential employers). The proposed system could help students in universities to increase their extra-curricular activities and improve non-academic skills. We designed the system based on the hybrid software structure model containing centralised and decentralised layers [125].

5.1 Contribution

The main contribution of this chapter is providing a conceptual design of a Blockchain-Based Trusted Achievement Record System and implementation.

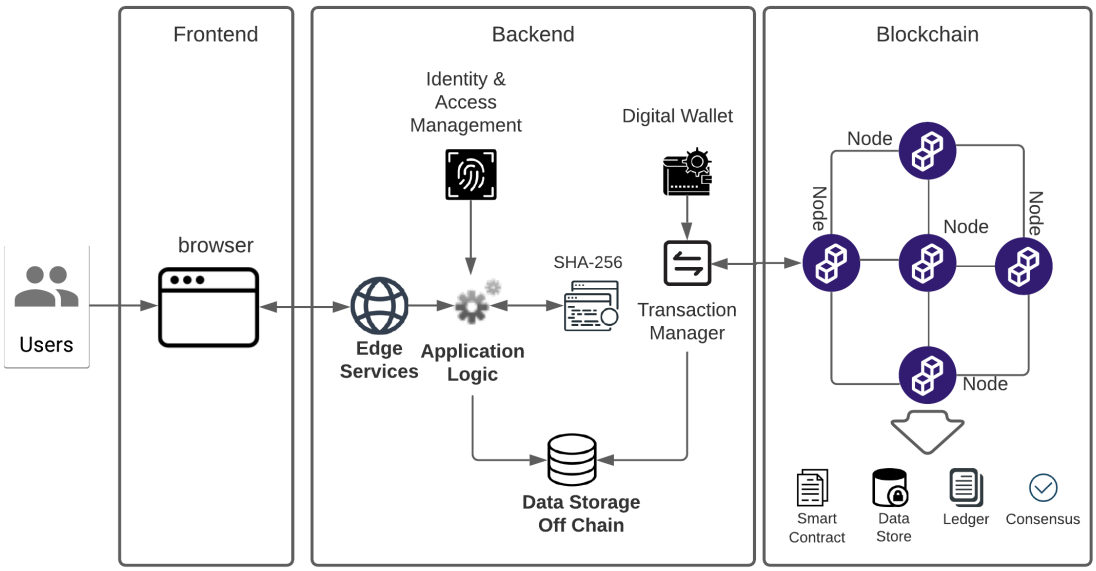


Fig. 5.1 System Structure

5.2 System Structure

The fundamental components of the Blockchain-Based Trusted Achievement Record System are consistent with use cases. We adopt the hybrid software structure described in Chapter 2 Section 2.2 to build our distributed system. Figure 5.1 illustrates the overall system design, and covers the previously discussed requirements and components including a frontend and backend. This architectural design signifies that there are two ends with separate set dependencies (libraries and frameworks). While the frontend acts as a presentation layer, being what the end-user sees upon entering the site, the backend provides the data and logic which enables the frontend to function.

Users. System users denotes any user who will access the system with their access information to complete tasks relating to an individual or organisational performance. The users in our proposed system are divided into two main categories: Admin and Regular user. Four users interact with the system. The first user is the system administrator, responsible for executing the smart contract on the blockchain and the registration of universities on the system. The second user is the university or learning institution, responsible for the authentication of student records. The third user is the student, who utilises the system to create a record of their achievements. The fourth user is an employer, who makes use of the system to validate the candidate's certification and assess candidates using their records

of achievements. To illustrate the interaction with the system and define the requirement to describe a particular use of the system, users will interact with the system in different ways.

Browser. A web browser (often abbreviated to browser), is a piece of application software that enables users to access the World Wide Web. When a user requests a web page from a particular website, the web browser obtains the required content from a web server and then displays the page on the user's device. A web browser's goal is to retrieve content from the Web and display it on the user's device.

Edge Services. Edge services typically enable a protected data flow from the Internet to the provider's infrastructure and then into the enterprise. Additionally, edge services can assist the backend by completing routine activities like authentication, authorisation and logging.

Application Logic. Application logic or domain logic, is the component of a programme that encodes the use-case rules that identify the creation, storage and modification of data. This component controls the interfaces of the system and their contents based on the type of use.

Identity and Access Management. Identity management (IdM), also known as identity and access management (IAM or IdAM), is a collection of policies and technologies that permit authorised users to access technical resources. The identity and access management component stores user data so as to authenticate users and provide data. This can be used by edge services to manage access to resources, services and applications on a per-user basis. As a result, it is critical for blockchain-based applications to align identity and access management comprehensively with the blockchain's core identity concept. Additionally, it must be specified how much user sovereignty over their blockchain identity is required and how this connects to application-wide identity management.

Data Storage Off Chain. Off-chain storage is used to refer to any data that is not stored on the blockchain yet contains blockchain-related data. Off-chain storage is required for two key reasons. On the one hand, local replication should enable faster access to data stored on the chain. Alternatively, it should keep business data separate from the blockchain, for security and scalability reasons. Off-chain storage can take several forms depending on the data type and size, for example, SQL or NoSQL for metadata or decentralised Content Addressable-Storage (CAS) systems, such as IPFS [16] or Swarm for Binary Objects (BLOBs) [122] that create hashes for data that can be stored on-chain.

Transaction Management. The transaction manager is a blockchain application service that is responsible for receiving messages and generating state-changing transactions that invoke smart contracts. It governs how transactions are signed and published to the blockchain network via a connected blockchain endpoint. The component is responsible for a range of transaction publication-related duties. To begin, it forecasts adequate transaction expenses to ensure that transactions are funded adequately and completed on time. Second, it keeps track of nonces; a nonce is a randomly generated number that is used to prevent replay attacks. Thirdly, it deals with the entirety of the signature for the transaction. Additionally, the transaction manager must deal with a range of probable errors, including nonce errors, network congestion, peers dropping, and transactions being dropped for whatever reason.

Digital Wallet. The wallet is a software component used to maintain encryption keys. It is necessary to provide the private key in situations where backend transactions must be signed. Numerous sophisticated approaches and various software solutions, such as HashiCorp Vault [102] and MitaMask [75], enable the secure storing of private keys on the backend. It stores and manages account keys, broadcast transactions, send and receive Ethereum tokens and connect to decentralised applications (API), so as to connect the frontend of the system to the smart contract on the blockchain.

Blockchain Endpoint. Blockchain endpoint is a node that runs software that implements the blockchain protocol. A node checks all transactions in each block, ensuring the network's security and data accuracy. The system's backend relies on the blockchain, a decentralised network of computer nodes that confirm and validate data added to the chain. This process hashes digital data blocks and adds them via a cryptographic link to the chain. Therefore, blockchain-based records are reliably easy and quick to transfer, with students only needing to share a digital address to link future employers to their authenticated credentials.

Smart Contract. A smart contract is a self-executing autonomous entity built on the blockchain to perform operations related to specified tasks. Smart contracts integrate the blockchain with the frontend of the system and it is written using Solidity [35] and deployed on the Ethereum Virtual Machine (EVM) on the blockchain. The smart contract combines with the frontend via the API.

5.3 Motivation Scenario

5.3.1 Initial Scenario

The following initial scenario involves four different actors. The first actor is the system administrator or sysadmin, responsible for the execution of the smart contract on the blockchain and the registration of universities on the system. The second actor is the university or learning institution, responsible for the authentication of student records. The third actor is the student, who utilises the system with the intention of creating a record of their achievements. The fourth actor is an employer, who uses the system in order to validate the candidate's certification and to assess candidates by way of using their records of achievements.

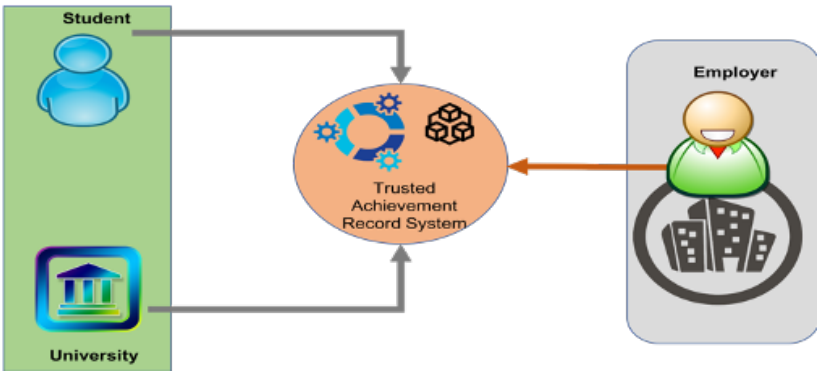


Fig. 5.2 Motivating Scenario

Each of these actors or users, interact with the system in different ways, according to a sequence. This is described below:

1. The sysadmin executes the smart contract on the blockchain. Following deployment of the smart contract on the blockchain, the sysadmin can register universities into the smart contract's storage. This function is one which can only be executed by the smart contract's sysadmin or in other words, executed from the address from which it was deployed. Figure 5.3 shows the admin sequence diagram.

2. The university name and address are stored in the smart contract utilised for the authentication of certificates. Figure 5.4 shows the university sequence diagram.

3. The sysadmin registers the university in the frontend of the system (meaning that the university name is added to the list of the universities registered in the smart contract).

4. Students can register themselves on the system via the system's homepage. Figure 5.5 shows the student sequence diagram.

5. The university adds students from the student's list in the system to its list.
6. Students added to the system now have access to the system with the use of an ID number.
7. Each time a university seeks to authenticate certificates, the relevant student is selected from the list.
8. Following this, the relevant documents are uploaded to the frontend, which hashes the certificate and calls to a function on the smart contract to ensure this hash is stored on the blockchain.
9. Following authentication of a student certificate, the certificate is automatically added to the student's record of achievements on the system.
10. When this occurs, the UI also sends an email to the student with a hash of the certificate.
11. Once provided with this hash, the student can send this certificate to their employer(s).
12. Once the employer receives this hash, they upload it to the UI for verification. Figure 5.6 shows the employer sequence diagram.
13. The frontend calls on a function in the smart contract in order to verify that the hash was authenticated by the university.
14. The true/false Boolean result is then displayed on the frontend, in the verifying window.

This motivating scenario demonstrates how data flow occurs within two different system platforms; it occurs off-chain in the frontend application and on-chain on the blockchain in the backend of the system.

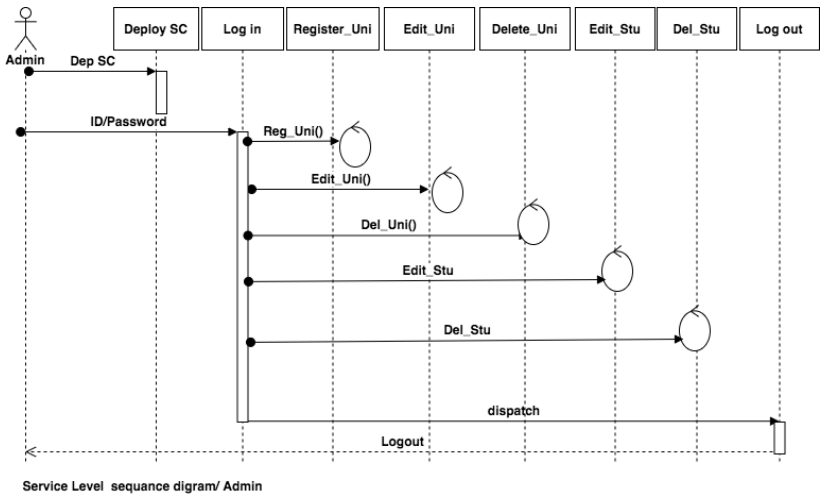


Fig. 5.3 Service Level sequence diagram: Admin

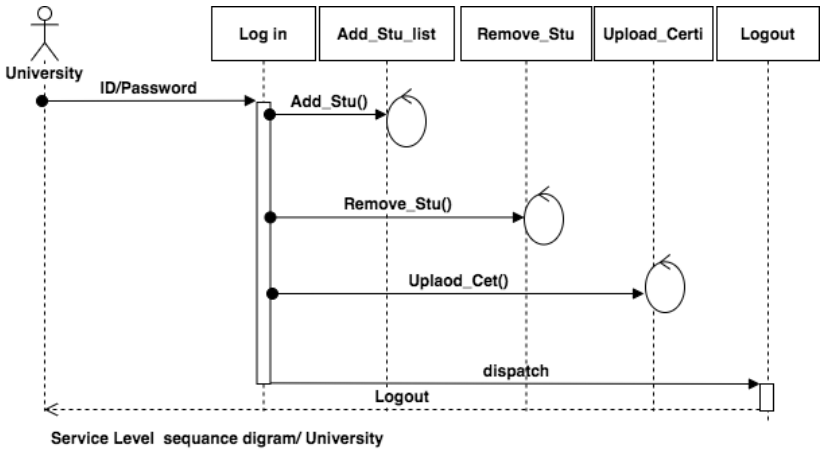


Fig. 5.4 Service Level sequence diagram: University

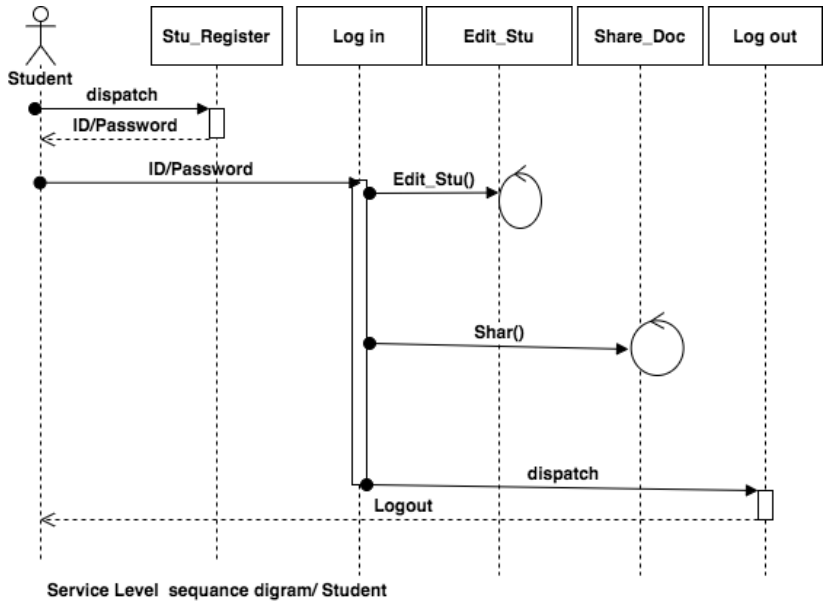


Fig. 5.5 Service Level sequence diagram: Student

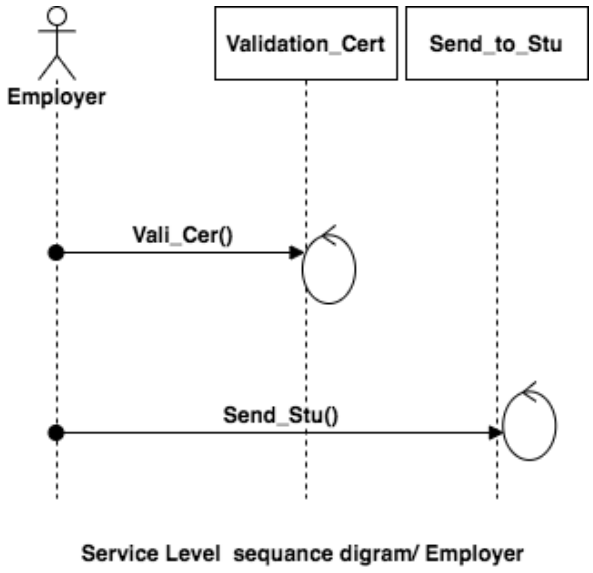


Fig. 5.6 Service Level sequence diagram: Employer

5.3.2 Scenarios for Analysing Special Requirements

The system must be designed in a way which makes it capable of coping with unexpected issues caused by the system itself or its users. Therefore, one primary necessity is the creation of scenarios for potential issues with the purpose of pre-empting issues and to formulate plans for their resolution. These issues might include faults within blockchain behaviour, user login and permissions.

Faults related to blockchain

One potential fault lies in the use of Ethereum Blockchain, which relies on miners for the verification of transactions, management of the network, the issuing of new Ethereum tokens and to secure the network. With an Ethereum transaction, the address of the smart contract is encrypted on the blockchain, alongside the certificate hash, the gas and the private key authorisation for verification of the side transaction. Ethereum miners will pick up transactions with the highest fees, signifying that miners will verify transactions with a high amount of gas more quickly. Likewise, it will take longer to achieve confirmation for a transaction with a low amount of gas. Additionally, enough Ether must be contained within the senders' digital wallets in order for the mining fee to be paid to the miners. This indicates that a scenario must be created so as to plan in the event of a "transaction not confirmed (verified) on the blockchain". However, this research does not intend to examine the technical faults relevant to blockchain or the consensus process.

Identity Authentication Issues

Any potential issues surrounding user authentication must be explored, as the privacy of the data is crucial. Only authenticated users should have access to information and not all users should have access to sensitive information. This implies that a piece of information must be given in order for a user to confirm their identity. Despite this measure, some issues with identity authentication are expected. To counter these issues, the system is designed to provide users with the ability to reset the information they use to access the system via a trusted and secure process.

5.4 Modelling Scenarios as Use Case

The primary purpose of requirement modelling is to correct the requirements of the proposed system. Scenarios are useful when discussing the purpose of the system, but the requirements

need to be specified more precisely before the system is fully designed. Accordingly, creating 'use cases' provides a detailed description, along with a model of the system.

Specification of Use Case

The specification of the use case includes:

- The name of the use case, which summarises its purpose.
- The actor/actors.
- The flow of events.
- Assumptions about entry conditions.

1. **Use Case 1: Log in**
   Name of use case: Login
   Actors: Admin, University and Student, see figure 5.7.
   Flow of events:
   (a) Actors open the system's main page.
   (b) Actors select the Login link.
   (c) Actors enter the ID and password.
   (d) The frontend of the system checks the information entered.
   (e) If the information entered is correct, then the access will be authenticated.
   (f) If the information entered is incorrect, then access will not be authenticated.
2. **Use Case 2: Log out**
   Name of use case: Log out
   Actors: Admin, University and Student, see figure 5.7.
   Flow of events:
   (a) Actors select the Log out link.
   (b) Actors accounts terminated.
3. **Use Case 3: Register University**
   Name of use case: Register University
   Actors: Admin, see figure 5.8.
   Flow of events:

(a) Admin login to the system (see Use Case1).

(b) Admin select 'Register University' link.

(c) Admin enter university name and address on Ethereum.

(d) Admin selects the option 'Add university'.

(e) Frontend call 'register_University' function in the smart contract that is executed on the blockchain.

(f) Admin confirm the transaction gas via the digital wallet.

(g) University information stored in the system's database.

Entry conditions:

(a) Admin must have an address on the Ethereum blockchain.

(b) Admin must have a digital wallet and sufficient Ether to pay for miners.

4. **Use Case 4: Delete University**
   Name of use case: Delete University
   Actors: Admin, see figure 5.8.
   Flow of events:

   (a) Admin login to the system (see Use Case1).

   (b) Admin select 'delete University' link.

   (c) Admin selects the option 'delete university'.

   (d) Frontend call 'delete_University' function in the smart contract that is executed on the blockchain.

   (e) Admin confirm the transaction gas from the digital wallet.

   (f) University information deleted from the system's database.

   Entry conditions:

   (a) Admin must have an address on the Ethereum blockchain.

   (b) Admin must have a digital wallet and sufficient Ether to pay for miners.

5. **Use Case 5: Edit University**
   Name of use case: Edit University
   Actors: Admin, University and Student, see figure 5.7.
   Flow of events:

(a) Actors select the Log out link.

(b) Admin select 'Edit University' link.

(c) Admin enter university name and address on Ethereum.

(d) Admin selects the option 'Edit university'.

(e) Admin can only edit the university name.

(f) University information updated on the system's database.

6. **Use Case 6: Register Student**
   Name of use case: Register Student
   Actors: Student, see figure 5.10.
   Flow of events:

   (a) Student selects the register link from the home page.

   (b) Student enter his/her information.

   (c) student submit the form.

   (d) System frontend will send an email to the student containing the user ID and password.

7. **Use Case 7: Add Student**
   Name of use case: Add Student
   Actors: University, see figure 5.9.
   Flow of events:

   (a) University login the system (see Use Case1).

   (b) University selects the option 'Add Student' from the menu and adds the student to its list.

8. **Use Case 8: Upload Certificate**
   Name of use case: Upload Certificate
   Actors: University, see figure 5.9.
   Flow of events:

   (a) University login to the system (see Use Case1).

   (b) University select 'Upload Certificate' link.

   (c) University enter Student name and Student ID.

   (d) Frontend presents the student's information on the page.

(e) University upload the certificate to the student.

(f) Frontend creates a fingerprint "hash" for the certificate.

(g) Frontend calls 'stor_hash' function in the smart contract to store the hash on blockchain.

(h) Frontend adds the certificate to the student's achievement record.

(i) Frontend sends a notifying email to the student's email.

Entry conditions:

(a) Admin must have an address on the Ethereum blockchain.

(b) Admin must have a digital wallet and sufficient Ether to pay for miners.

9. **Use Case 9: Delete Student from the university list**
   Name of use case: Delete Student
   Actors: University, see figure 5.9.
   Flow of events:

   (a) University login the system (see Use Case1).

   (b) University select 'Student' from the list.

   (c) University select 'Delete Student' link.

   (d) Frontend removes the student from the university list.

10. **Use Case 10: Edit Student**
    Name of use case: Edit Student
    Actors: Student, Admin, see figure 5.7.
    Flow of events:

    (a) Actors login to the system (see Use Case1).

    (b) Student select 'My Profile' from the list. Admin select the student's name from the student list.

    (c) Actors select 'Edit' link.

    (d) Frontend updates the student information on the system's database.

11. **Use Case 11: Check Record**
    Name of use case: Check Record
    Actors: Student, see figure 5.10.
    Flow of events:

(a) Student login to the system (see Use Case1).

(b) Student selects ‘Documents list’ link.

(c) Frontend shows the student achievement list.

12. **Use Case 12: Validate Certificate**
Name of use case: Validate Certificate
Actors: Employer, see figure 5.11.
Flow of events:

(a) Employer open the system main page.

(b) Employer select ‘Access Achievement Record’

(c) Employer posts the link received from the student.

(d) Employer selects ‘See the record’.

(e) Frontend shows the student achievement list.

(f) Employer downloads certificate.

(g) Employer selects ‘Validating’ option.

(h) Employer uploads the certificate to the system.

(i) Frontend creates a fingerprint for the certificate.

(j) Frontend calls ‘check_hash’ in the smart contract.

(k) The function matches the hash with the stored hashes on the smart contract.

(l) The function returns the name of the university and its address on the blockchain if the hash exists.

(m) The function ‘not valid’ if the hash does not existing.

5.4.1 Use Case model

System Use case Model

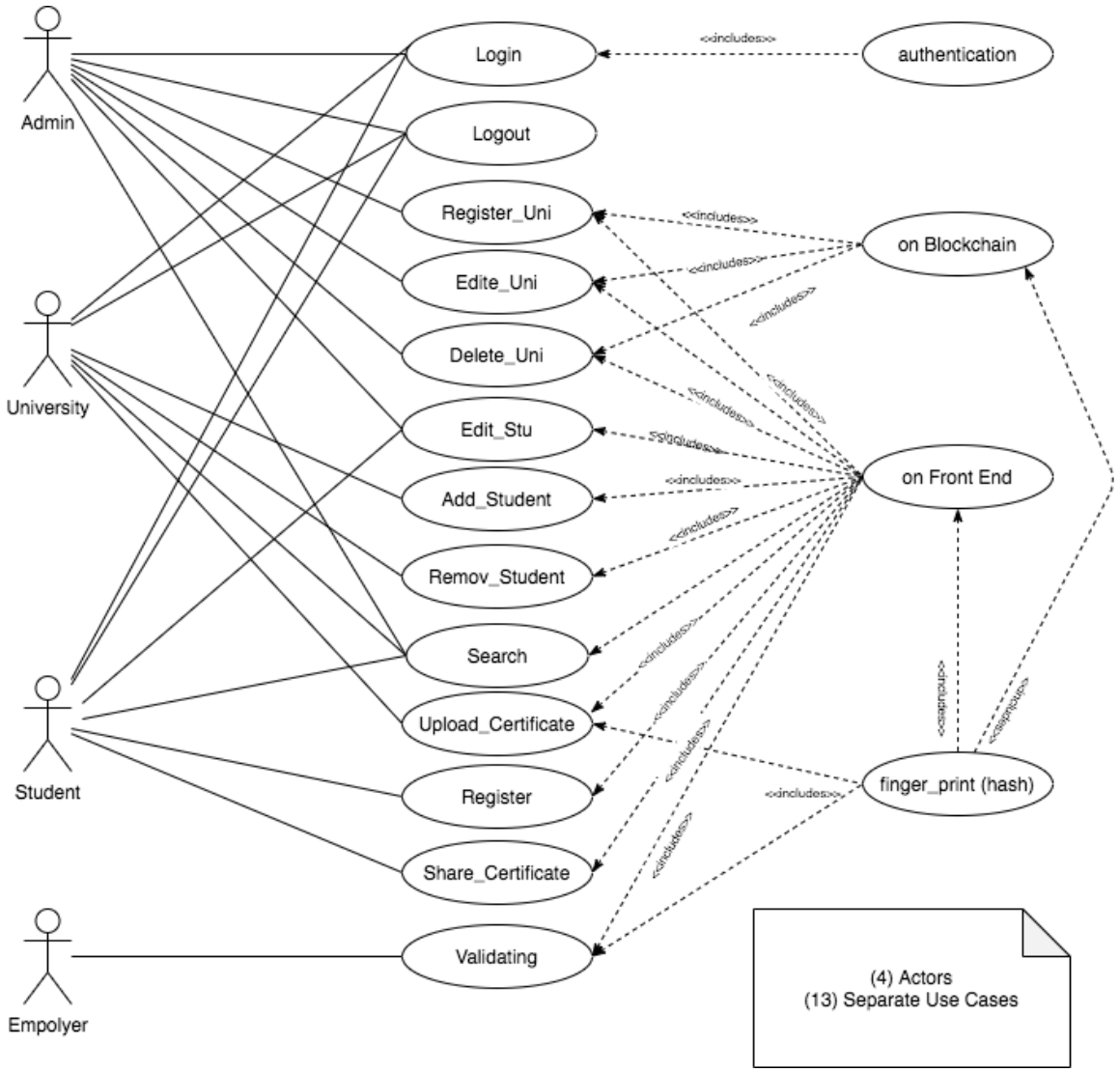


Fig. 5.7 System Use Case Model

Admin Use Case Model

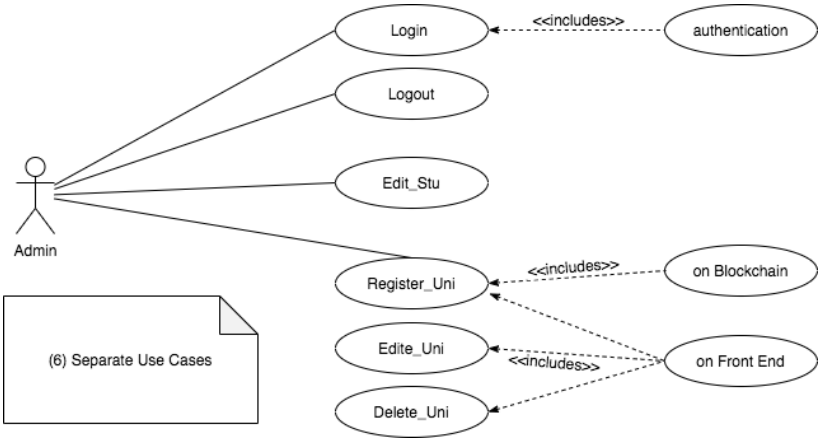


Fig. 5.8 Admin use case model

University Use Case Model

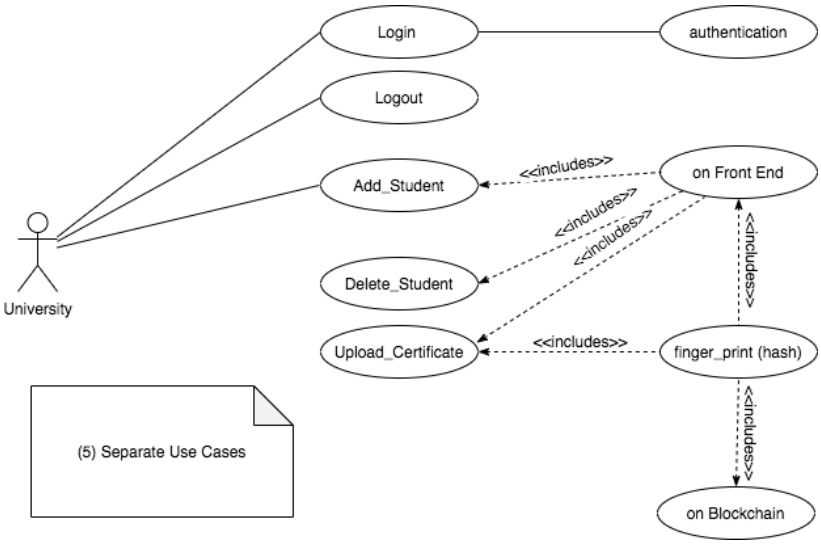


Fig. 5.9 University use case model

Student Use Case Model

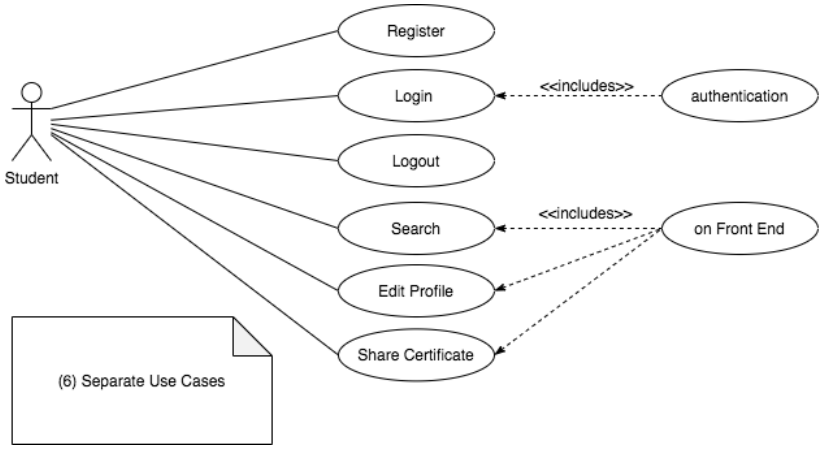


Fig. 5.10 Student use case model

Employer Use Case Model

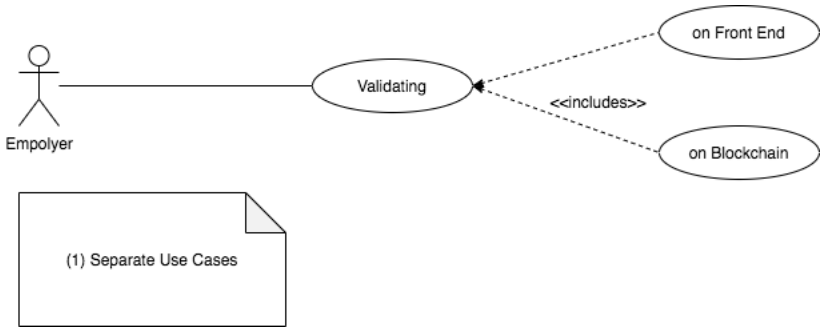


Fig. 5.11 Employer use case model

5.4.2 Entity Relationship Diagram (ERD)

An Entity Relationship Diagram (ERD) is a type of flowchart in this diagram, that illustrates how “entities” such as universities, students or employer relate to each other within a system. ER diagrams are most often used to design or debug relational databases in the field of software.

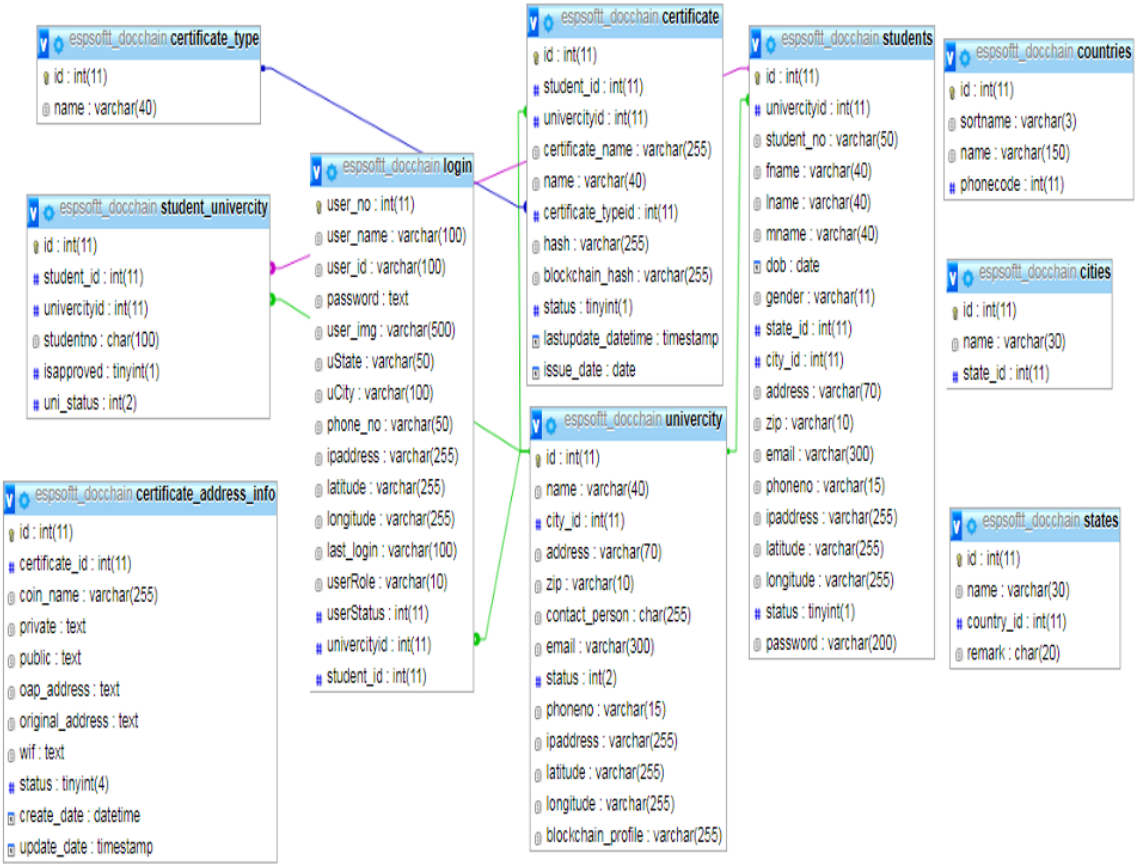


Fig. 5.12 Entity Relationship Diagram (ERD)

5.5 Dataflow

Dataflow automates provisioning and management of processing resources to minimise latency and maximise utilisation so that you do not need to spin up instances or reserve them by hand.

The flow of data for student

This flow diagram 5.13 represents Student activities in this system. First, the Student will login to the System with User ID and Password. If the information entered is correct then they will be able to redirect to Dashboard. If he/she fails then he/she will see an error message in the same login page. In dashboard, the User can find the list of certificates uploaded by Universities and can see their information. Students can share documents to Employers via Email. Student can view and update his/her profile and logout from this System.

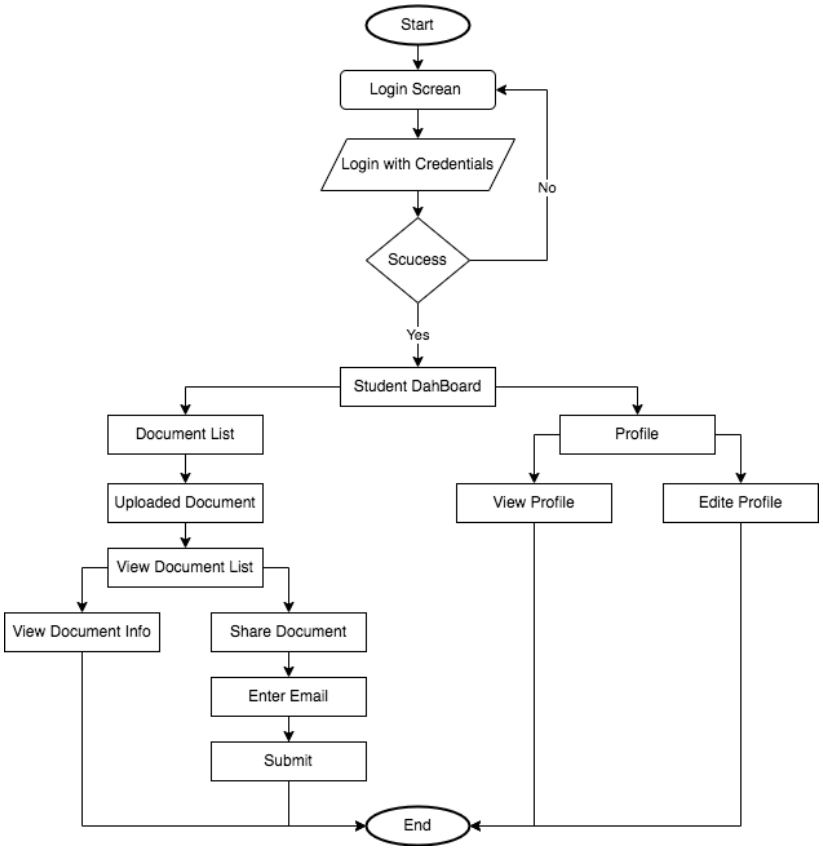


Fig. 5.13 Student Dataflow

Flow of data for the University

This flow diagram 5.14 represents the flow activities of the university in the system. First the university will log into the system using its login credentials. If the credentials are correct then the university user will be redirected to the university dashboard on dashboard user and will see the menus-document list, Upload Document, Add Students, manage students. In 'document list', the university user will be able to see a list of the student's documents. On clicking on any of the documents, the user will be able to view information in relation to the student. In the 'Upload document page', the university user can upload the document belonging to the student by entering their details. If document type is available in the system then they can directly upload the document. If it is not available, they need to add document type and then they will be able to upload the document. On the "Add student screen", the university user can add a new student with the full details and save it in the database. On the 'Student manage Screen', the University user will be able to see the full list of students and can edit and delete them.

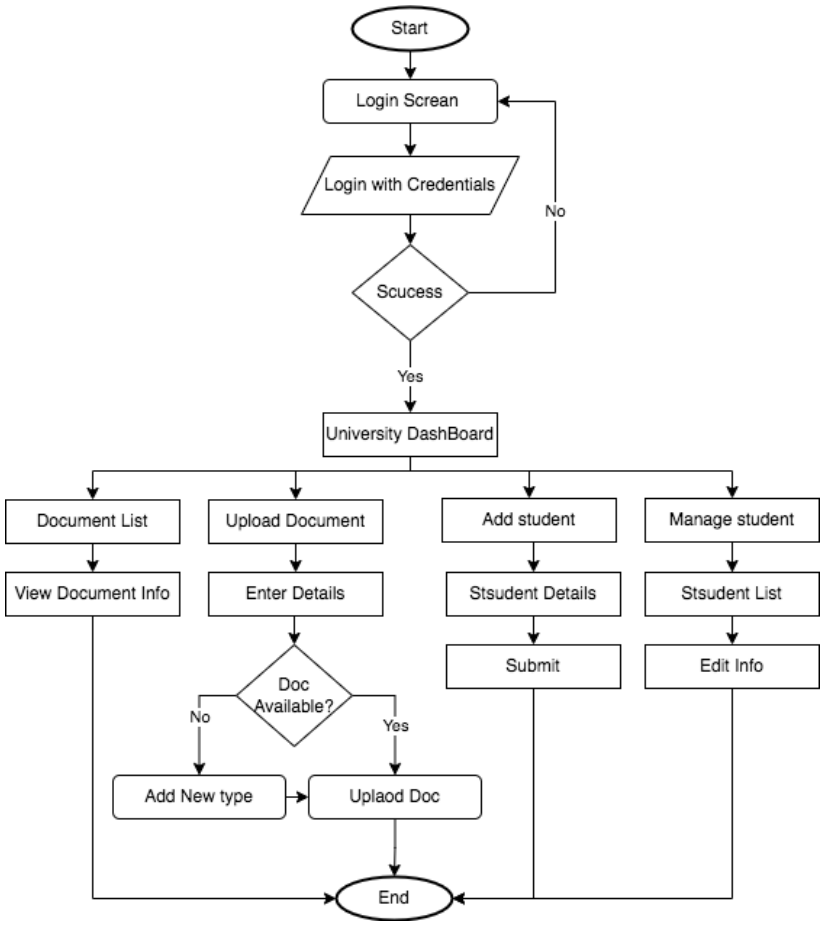


Fig. 5.14 University Data Flow

Flow of data for admin

This flow diagram 5.15 represents the Admin's flow activities in the system. First, Admin will login to the system with their login credentials. If the credentials are correct then admin will be redirected to the admin dashboard on dashboard admin and will see the menus - Add University, Manage University. On the 'Add university Page', admin can add the university in the university database by adding the correct details to the form. In addition, on the 'Manage University' screen, admin will be able to edit and delete universities.

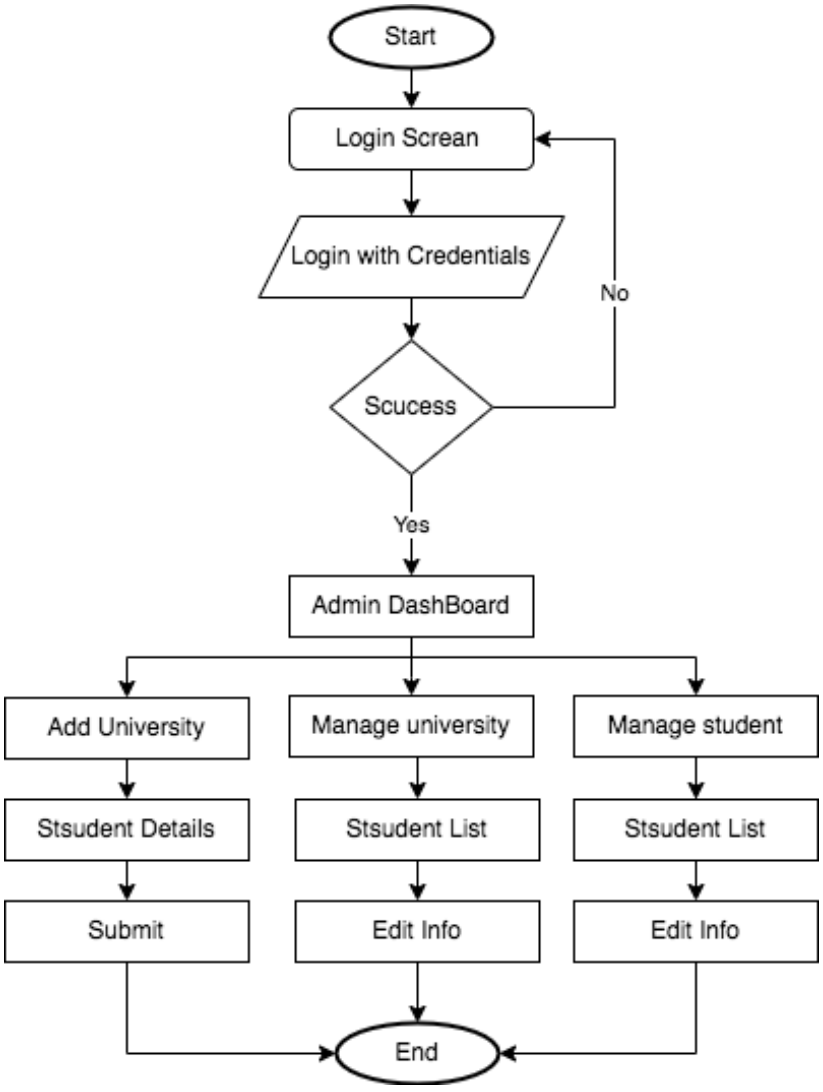


Fig. 5.15 Admin Data Flow

Flow of Data for Employer

This flow diagram 5.16 represents the employer's flow activities. The Employer will receive a link via an email sent by the student. On clicking on the link, the employer will be able to see the documents for verification.

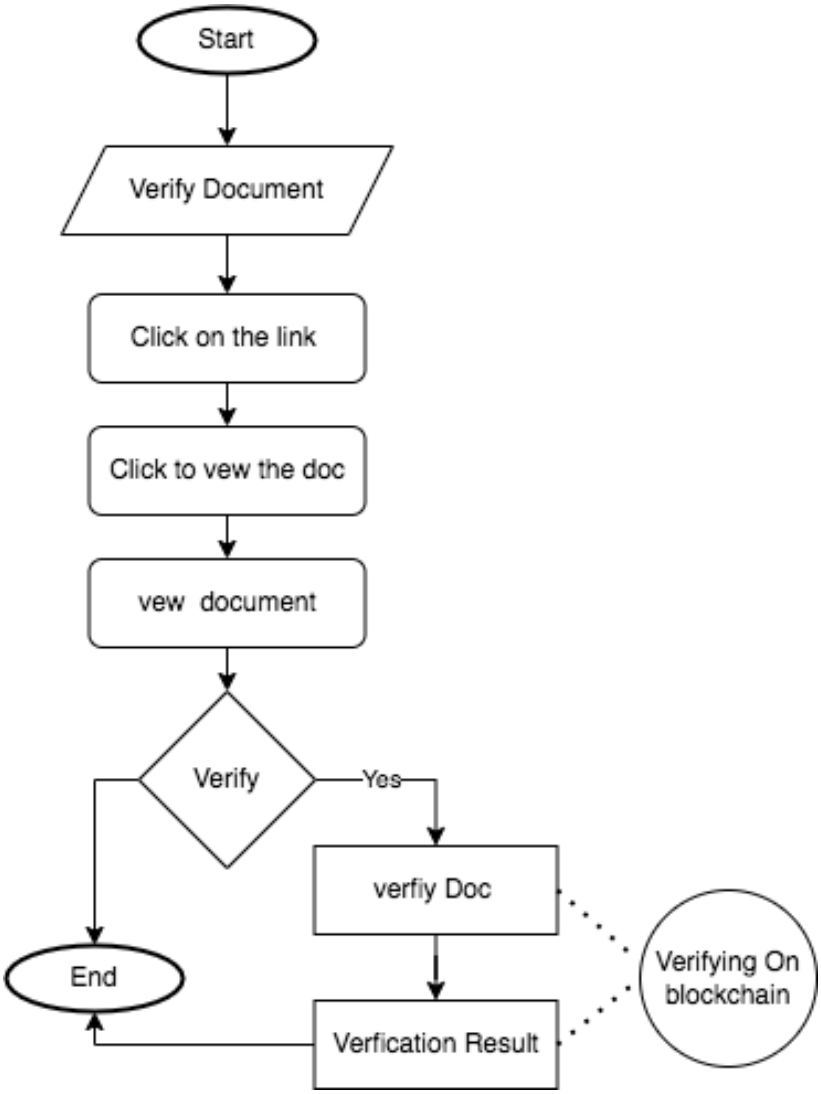


Fig. 5.16 Employer Data Flow

5.6 Validation of the Conceptual design

5.6.1 Method

We investigated the validity of the conceptual design of the prototype prior to the implementation through *a design critique workshop* for multiple reasons. First, it yields valuable feedback quickly and regularly. Second, it allows people to provide direct constructive feedback on the design. Third, it builds resilience in the designer to be open to criticism of their work and thus improve its quality. We conducted a qualitative questionnaire besides participants ' recorded and written feedback to collect valuable data to validate our proposed solution and build the system. In addition, the recommendations have addressed the comments, suggestions and advice of the participants. To achieve our aim, we designed the workshop using the "Six P's" [47] framework (See Table 5.1) to manage the quality of the process [131]. The participants were compensated with a £10 Amazon gift card for their participation [32] [27].

Table 5.1 Six P's workshop framework.

Purpose	Participants	Principles	Products	Place	Process
Why do we do this workshop?	Who is involved?	How do we function?	What do we do?	Where is it located?	When is the meeting?
To validate the conceptual design of the proposed solution	Blockchain Developers /experts, HCI Developers/experts, Stockholder.	Group process rule. Meet the group and discuss the design. Answering the questionnaire. Individual interview.	Discussion. Planning. Modelling.	School of Computing, Newcastle University, Meeting Room.	29/11/2019 From 10:00 am To 12:00 pm

We invited eight people via email, as recommended in [32], to participate in the workshop via email **(see Appendix A for the invitation designed for this study)**. Therefore, the process is efficient since we need a few numbers of specific types of participants. The workshop was composed of a mix of developers and stockholders. Participants were active, engaged and committed. Table 5.2 presents information regarding the participants.

Table 5.2 The workshop participants' details.

Participant	Education Level	Participants fields
P1	PhD	Blockchain
P2	PhD	Blockchain
P3	PhD	Blockchain
P4	PhD	HCI
P5	PhD	HCI
P6	PhD	HCI
P7	PhD	Software Engineering
P8	PhD	Software Engineering

We conducted an in-depth explanation of the purpose of designing a trusted achievement record system for students in higher education using blockchain and smart contract technology. To deliver the idea to the participants, we created an infographic storyboard of the research idea that we presented as a video and a printed story **(see Appendix A)**. Then, we answered the questions listed in the Agenda section in detail to understand the components, method and scenario that we incorporated into our solution. Participants were recruited using three specific approaches to give their feedback on the design of the prototype.

The first was by way of attending the workshop meeting and discussing their opinions in an open discussion session. We arranged a meeting; the discussions were recorded using an audio recorder in the middle of the meeting table. The discussion session allowed the participants to ask direct questions and provide immediate comments and suggestions.

The second was by using sketching papers to allow the participants to write and draw their ideas and thoughts. Thus, we can map the concepts into categories and improve the prototype.

The third approach was sending a short quantitative questionnaire, conducted using 'SurveyMonkey' software, to the participants via email**(see Appendix A for the questionnaire)**. The primary aim was to collect valuable data from the participants that reflected their opinions and thinking regarding the workshop discussion. We analysed the results using basic descriptive statistics and specific cross-tabulations.

The discussions were transcribed and then coded to identify the components. A code is a word or short phrase that descriptively captures the essence of the components of our material. The first step in our data reduction and interpretation was coding the materials. Therefore, transcripts were coded to transform the data into relevant information. Our study followed a thematic analysis using the inductive approach [22], an effective method in such investigations and used in many similar studies previously'[131]. The second step was abstracting themes from the codes. Once we coded all of the materials, we worked on the codes to group them together to represent common and significant themes. We used the 'table method', which works particularly well in this study, for cutting out codes, as well as for moving them around and grouping codes.

5.6.2 Results

The findings of the activities observed during the workshop meeting and from the questionnaire were disseminated via email. Primarily, we classified the participants' comments under four main categories as follows:

Usability

Usability can be defined as the ease associated with using the system effectively and efficiently. Usability is one of the primary targets that we are looking to achieve and requires a comprehensive understanding of the requirements and components. Integrating the components in our solution is essential and should be completed in a way that allows users to feel comfortable while dealing with our system. Our system is designed to demonstrate the research idea at the current stage. Therefore, the system's usability in the current arena is suitable according to the participants' answers to the question (How satisfied are you with the usability of this software?) (see Figure 5.17).However, we asked the participants how satisfied they were with the system's usability. The result shows that 37.5% of the participants were somewhat satisfied. From their perspectives, the system's user interface needs a variety of improvements to be more friendly. According to (P7), *"the end-user must not have any concerns about how to use the system and they must see it like any other system they use every day"*. A further 37.5% of re were very satisfied with the system's usability, while 25% were extremely satisfied. *"MetaMask solution is good for proof-of-concept but is not good to evaluate usability. Consider using some web3 library (web3js, web3dart, etc.) to communicate with Ethereum blockchain"*, (P1) said.

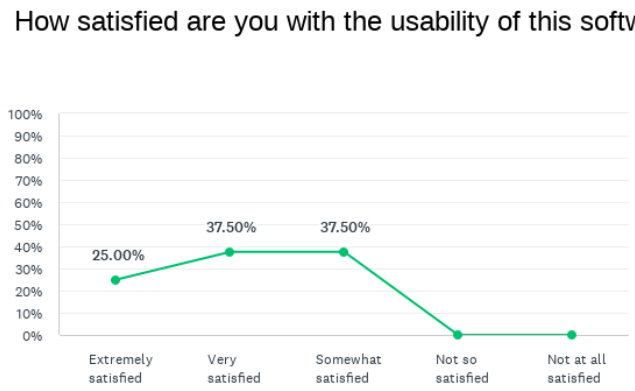


Fig. 5.17 Participants' Satisfaction with the Usability.

Scenario

To understand the system requirements and how they are applied, it is essential to compose a scenario in the system's planning stage. We improved the initial scenario we produced in our solution as a result of the participant's feedback regarding the scenario. Figure 5.18 shows that the majority of participants,75%, were very satisfied with the initial scenario, while 25% were extremely satisfied. However, during the discussion in the workshop meeting, participants offered suggestions and feedback that would be used to improve the scenario. For example, two participants (P1) and (P2) suggested allowing the university to hash/sign the certificated and send the hash to our system instead of hashing certificates in our system. According to (P1) *"The scenario is relevant and blockchain can be useful"*. However, as we discussed, maybe you can improve it by allowing the institutions to hash/sign the files to send to external storage (external database, IPFS, etc.)' while (P2) believed *"It would be better to leave the hashing work to the university side. Likewise, using public blockchain is a good idea."*

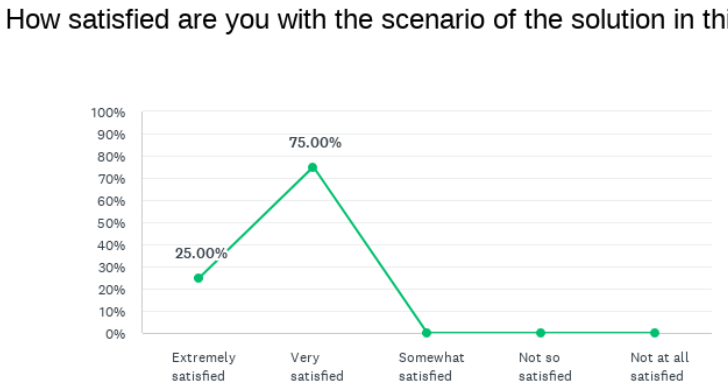


Fig. 5.18 Participants' satisfaction with the Scenario.

Moreover, (P7) suggested allowing students to access the system and manage their achievement records *"Students must have the ability to access the platform and manage their achievement records. Then they don't have to send their certificates by email to employers; they can only send their record link"*. Another suggestion to improve the scenario from (P4) is to allow students to communicate with the employers through the system and vice versa. *"The scenario could be improved by: 1. Increase the level of security, especially regarding the company. 2. Automated handling and storing a document on the system. 3. There is no need for communication between the document owner and the authority as long the document is available automatically.'"*, (P4) said.

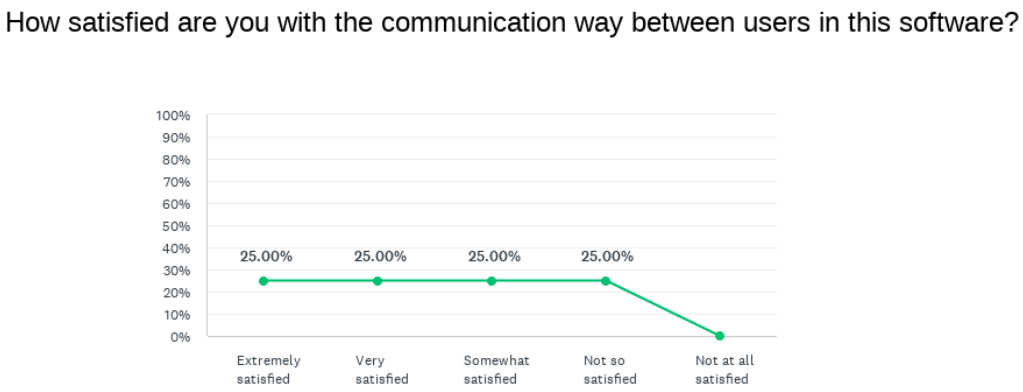


Fig. 5.19 Participants' satisfaction with the communications between users.

Security

Blockchain in the backend provides a secure and trusted environment for our system. However, the system's frontend should be protected so users can use this system confidently. To raise the level of security in our solution, we designed a question in the questionnaire that aims to indicate if the participants were satisfied with the system's security. The result shows that 37.5% of the participants were not so satisfied. Alternatively, 37.5% of the participants were extremely satisfied, while 25% were in between somewhat satisfied and very satisfied. Participants (P1) and (P2) argued about moving the hash/sign certificate process

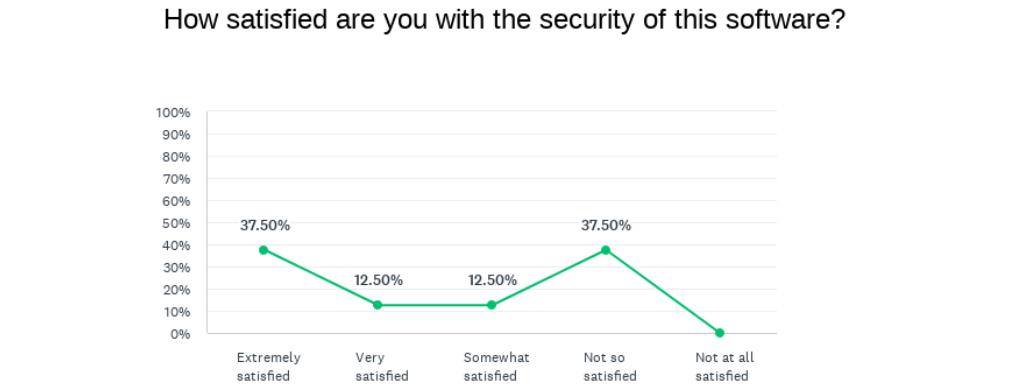


Fig. 5.20 Participants' satisfaction with the Security.

from the system to the universities to avoid the possibility of security issues related to the hashing method itself. *"As we discussed, institutions needed to be capable of performing the hash/signature. Therefore, it will not rely on third party trust (blockchain was designed to*

remove the requirement of the third-party trusted entity)" (P1) said. Considering the same idea, (P2) said that *" Using the trusted hash function and let the universities undertake most of the work."*

With respect of protecting users' identities and data, (P3) and (P7) had a common recommendation which is defining the users of the system and determining their tasks. *"With the scenario that I was shown, it would be incredibly difficult for anybody to forge or alter any documents, the only potential threat I see is that the blockchain currently requires an administrator to oversee the management of the chain if this role was decentralised, I think that would improve security further."* (P3) said. While (P7) said, *"The prototype needs some improvement in the security layer. For example, determine each user's tasks and protect their identity."*

Last, in the security section, signing the permissions of each user is an essential step while designing any system. Therefore, (P6) argued that users of the system should not be allowed to see all the system windows. The permission of each user of the system should be related to the user's tasks. 'Implement a security layer between the database and presentation layer. "The other concern regarding the security is that the users shouldn't see all options/screens belonging to the system." (P6) said.

Components

All processes are placed into separate components in our system. Thus, all the data and functions inside each component are semantically related. Components communicate with each other via the system's interface. Therefore, the user does not need to understand the inner workings of the component (implementation) in order to use it. The system we are designing contains various components with different characteristics. For example, blockchain and smart contract at the backend of the system and a frontend that includes a database, hash method and security layer. Combining the components in good content is one of our interests that we are seeking to achieve. Therefore, we conducted some questions relevant to the components of our system, such as blockchain, smart contracts and the hash method. We first discussed the question (How satisfied are you with conducting the blockchain and smart contract in this solution?). Figure 5.21 shows that the majority of participants, 50%, were very satisfied while 37.5% were extremely satisfied. Only 12.5% of the participants were somewhat dissatisfied. After explaining the technology, we investigated which blockchain type the participants thought might be best to apply in this solution. Figure 5.22 75% chose public blockchain, while 25% chose private blockchain. We also asked the participants the direct question (How satisfied are you with including (public-blockchain) in this solution?). The result presented in the Figure 5.23 shows that, the majority

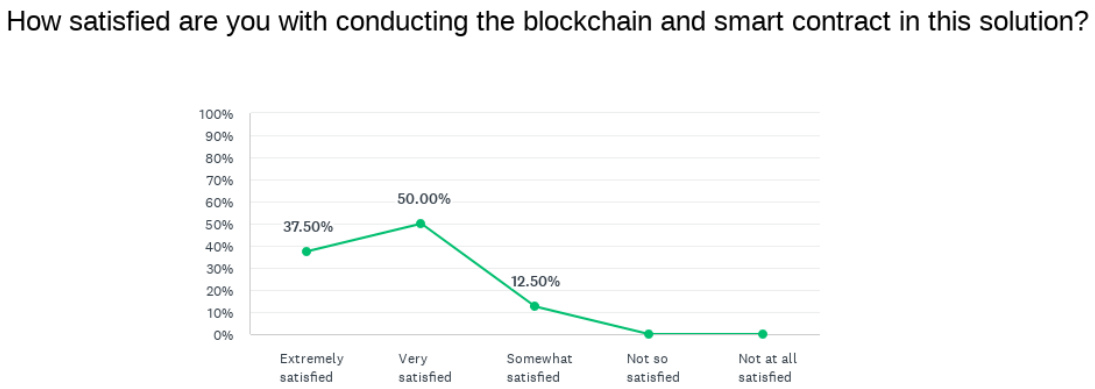


Fig. 5.21 Participants' Satisfaction with the Components.

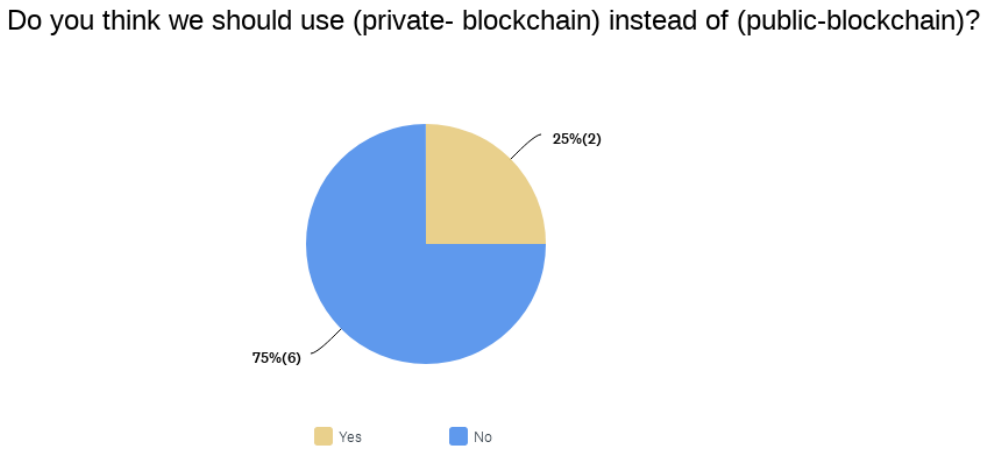


Fig. 5.22 Participants' Selection of the Blockchain Type.

of participants 50% were extremely satisfied with using a public blockchain while 37.5% were very satisfied, whereas only 12.5% were somewhat satisfied. Participants provided

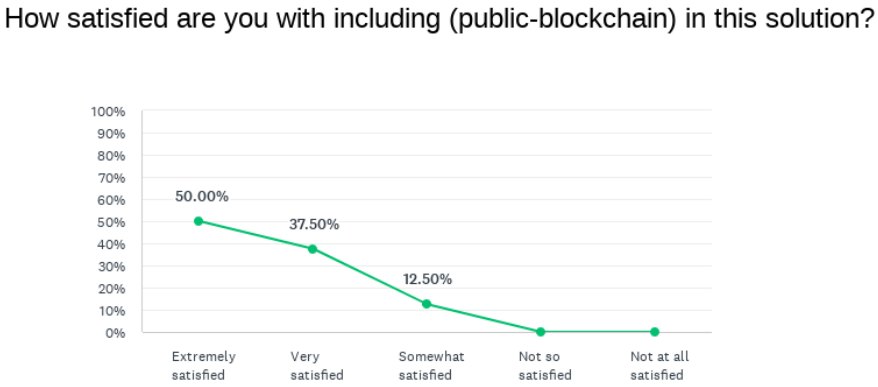


Fig. 5.23 Participants' Satisfaction with the Blcokchain Type.

justifications for their choices. (P1) said, *"About private/public instance, It depends on how the final design will be established. Various questions should be made to define this: - Would the entities involved in the blockchain pay for the infrastructure cost? (yes - private can be a good option) - Would nodes be able to pay the costs of transactions (gas)? (if yes - the public can be a good option) - Is it required for the solution to have some control over the access to the information available/stored in the BC? (if yes, consider using a private)"*. Participants (P3) and (P7) shared the same reason. *"Since the hash is the only data that will be stored on the blockchain, it is believed that Public blockchain is better (so you do not have to be concerned about miners and the consensus algorithms)"* (P3). At the same time, (P7) said, "I think public blockchain offers more security, and if only hashes are being stored in the chain and not personal information, this solution would be fine".

Another question we discussed in the workshop was relevant to the hash method. We explained the reason for using it in this system to the participants. Regarding the results of our question about how satisfied they are with making use of the hash method in this solution, 37% of the participants were extremely satisfied while 25% were very satisfied. 25% of the participants were somewhat satisfied and finally 12% were not satisfied,as Figure 5.24 illustrates.

5.6.3 Discussion

The primary aim of this study was to collect useful data to validate our proposed solution in order to implement the system. Therefore, the findings of this study revealed the main

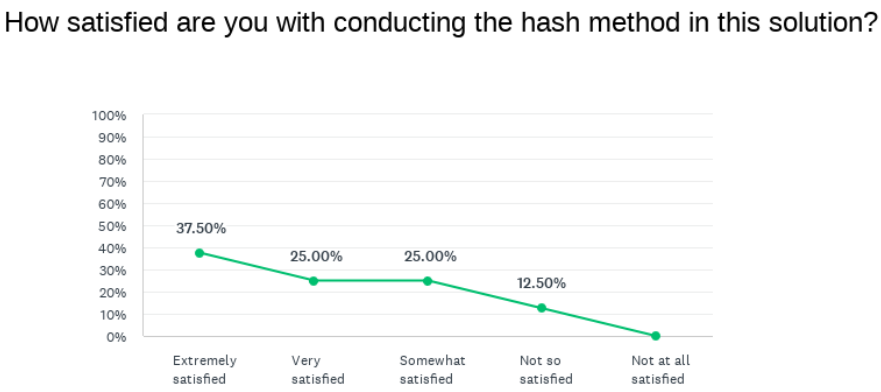


Fig. 5.24 Participants' Satisfaction with the using Hashing Algorithms.

factors illustrated in Section 5.6.2. In the planning and designing stage of the system, the main objective was to make the system easy to be used by the end-users; the user does not need to know about the inner workings of the system. As a result, the usability of our system in the current stage was highly satisfactory.

The first step in the validation process is reconstructing the scenario to cover the system requirements. After reviewing the participants' feedback related to the scenario, we determined that the tasks and permissions of the system users necessitate being redefined. Therefore, we redefined the tasks, which resulted in a redesign of the system's front end to serve the objective of the system, which is building a trusted achievement record for students. Fundamentally, improving the scenario is by going through these steps in sequence: defining the system users, determining the tasks for each user, selecting the appropriate components and lastly, illustrating the transactions and operations.

Moreover, system security is an essential part of this study. The study results in section 5.6.2 illustrate several issues related to the security of the system that should be addressed in the improvement process. Our findings reveal that the security layer in the system must be developed by adding security operations and features. The backend of the system contains the blockchain, which is secure by design, and the smart contract running on it is designed to be secured. Conversely, the frontend of the system needs to be more secure. The users' identities must be protected and the permissions for each user must be identified as well. Besides, the inner elements of the system must be secured from any external influence. Therefore, we addressed those points as a significant assignment to build a trusted system and refined the design based on the comments. In addition, other comments in the results discussed the components chosen while designing this system. The discussion among the participants and their answers in relation to their satisfaction with the system components

shows that we integrated suitable components in our solution. Therefore, there is no need to change any element in this system during the improvement process.

5.7 Conclusion

In conclusion, this chapter and the chapter 6 next, the following research questions in Chapter 1, page 5 and 6; were answered:

- **How can the documents be verified using blockchain and smart contract technology?**
- **How can each user's (students, educators, etc.) operations and transactions be specified in our proposed solution?**
- **What are the modelling scenarios of the system use cases?**
- **What are the modelling scenarios of the data flow?**

This study provided the data needed to validate the conceptual design of the proposed system. The scenario, security, components and usability are the four main factors discussed and validated based on the participants' answers and discussion. Therefore, we refined the design based on the results in the section to build a trusted and secured achievement record for students. The system, as a result has proved the effectiveness and validity as a solution for students to develop a trusted record of their achievements during their university life. The next chapter covers the details related to implementing the proposed conceptual model.

Chapter 6

Blockchain-Based Trusted Achievement Record System Implementation

Overview

The main aim of this chapter is to provide information on the implementation of the proposed system based on the design discussed in chapter 5. Moreover, this chapter presents details of the end-user interaction with the system.

6.1 Contribution

The main contribution of this chapter is providing information about the Blockchain-Based Trusted Achievement Record System implementation and verification.

6.2 System Implementation

The system built on the basis of work published in [11] and [12] (chapter 3 and chapter 4). The frontend of the system is software implemented using HTML5, CSS3, Javascript, AJAX and Web3js [75]. We used HTML5 to design the frontend application. By using HTML5, we made usable forms. In addition, HTML5 supports cross-platform, is designed to display the application pages on PCs, Tablet and Smartphones and ensures that CSS is better organised. Javascript is use to allow users to interact with the system frontend and to implement the frontend components. AJAX was used in this platform to allow a web page only to reload those portions which have changed, rather than reloading the whole

page. This decentralised application is connected to a smart contract using web3js. Web3js is a collection of libraries that allows users to interact with the local or remote Ethereum node using an HTTP connection. The database has been designed to contain two categories of data: public authentication data and private certificate data. The public authentication data is available and released to the blockchain; the student data are stored in MySQL, securely protected and isolated in the intranet. The smart contract in this system is written by Solidity [126], a high-level and contract oriented language used to write smart contracts. It is used for designing and implementing smart contracts. It is designed to run on the Ethereum Virtual Machine (EVM), which is hosted on Ethereum Nodes connected to the blockchain.

6.2.1 Blockchain

A blockchain-based application has been chosen for this system due to its performance and ability to verify education certifications proficiently. There are numerous reasons why blockchain is the most appropriate decision, including because it helps to remove the need for the manual verification of transactions since all necessary information is automatically verified by a decentralised network of computers. This information is also permanently stored in the blockchain, reducing, if not completely removing, the risk of deletion, meaning that additional security services are not necessary. Crucially, the falsification or modification of transactions on the blockchain cannot take place. The specific hash system is used to verify certificates. Furthermore, no user is capable of modifying this information or uploading a false hash into the network. When data is added to a blockchain, a request for the exchange of data is given by the sender and received by one of the nodes in the blockchain. The receiving node then broadcasts the incoming data to other nodes, adding it to the current transaction pool. When the block's limit is reached, determined by either the size or number of units, the nodes begin mining the block. The nodes compete to identify the proof of work solution, and when one of the nodes succeeds in mining, the solution is transmitted to the other nodes. The other nodes are responsible for verifying the output and assessing its validity before all blocks in the chain are verified and the newly mined block is added. The blockchain used for this specific system is Ethereum, an open-source blockchain with smart contract capabilities. It also supplies a decentralised virtual machine that can complete the necessary scripts through the use of a system of public nodes. This system is considered to be Turning complete, meaning it can recognise other data sets and is also used as the internal transaction pricing mechanism. Decentralised applications are connected to the smart contract using web3.js, which is an assortment of archives that permit the system to interact with remote or local Ethereum nodes [26].

6.2.2 Smart Contract

The smart contract is of primary importance within the system, as it connects the blockchain with the frontend [86][85]. Regarding this specific platform, the use of a smart contracts eliminates the need for human management using an Application Programming Interface (API).

The primary programming language used when writing smart contracts that run on Ethereum Blockchains is Solidity [126], a contract-oriented language that is responsible for the secure storage of programming logic during a transaction. Solidity [126] is also a high-level language and is used in the design, writing and implementation of smart contracts to run on the Ethereum Virtual Machine (EVM), which is held on Ethereum Nodes that are directly linked to the blockchain, that in turn is connected to the frontend. A smart contract

```
function add_uni(string _name, address addr) onlyOwner public {
        data[addr].userAddress = addr;
        data[addr].name = _name;
    }
```

Fig. 6.1 Adding University Function in the Smart Contract.

allows this platform to register universities and store the relevant document hash values on the blockchain, with Solidity [126] and Truffle Framework working to publish it on the Ethereum Blockchain. It employs automatically when a command is given on the frontend via API connectivity. First, universities are registered on the blockchain using an API with the

```
function store_hash(string _hash, address addr) onlyOwner public {
        data[addr].hash.push(_hash);
    }
```

Fig. 6.2 Storing the Document Hash Function in the Smart Contract.

formulated function *add_uni*; Figure 6.1 Another formulated function, *store_hash*; as seen in Figure 6.2 works to store the relevant document in the smart contract and was generated by the SHA-256 encryption algorithm that exists in the system's frontend. The function *get_hash*; in Figure 6.3 is employed to verify particular documents on the hash through an API.

```
function get_hash(address addr) public view returns( string[] _hash) {
        _hash = data[addr].hash;
    }
```

Fig. 6.3 Verifying the Document Hash Function in the Smart Contract.

Verification of the Smart Contract. The verification stage is a debugging task that primarily guarantees the smart contract is free of errors and capable of performing the functions specified in the model. The verification process identifies and correct errors in the early phases. To do that, we used Remix [72], an online integrated development environment IDE, as shown in the Figure 6.4, to test all the functions in the smart contract and ensure they all are delivering the correct outputs.

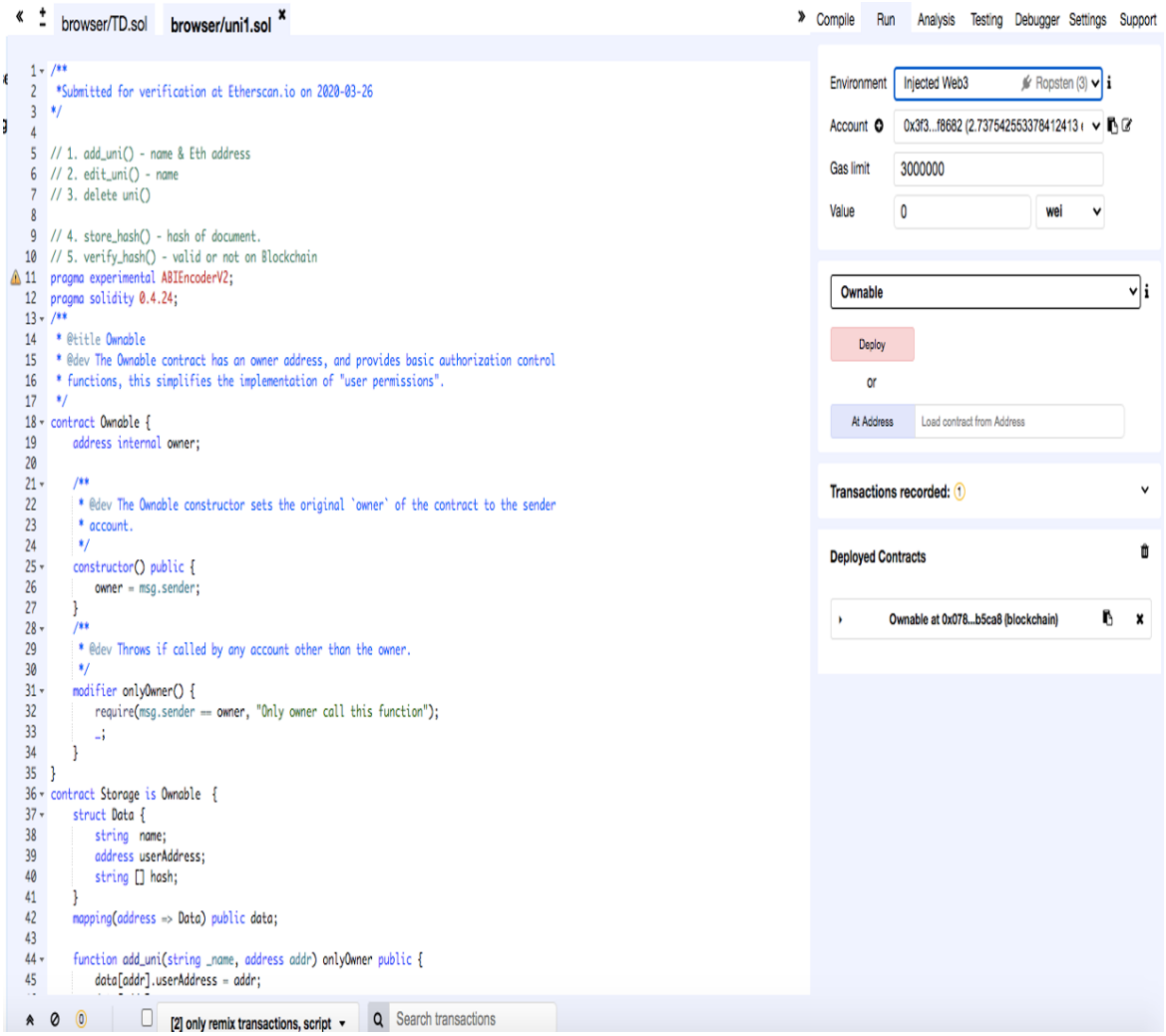


Fig. 6.4 Verification of the Smart Contract.

6.2.3 Hash Algorithm

In 2000, a cryptographic hash function was propositioned as a new production of SHA functions and was employed under the Federal Information Processing Standards (FIPS) in 2002. Named SHA-256, it is typically viewed as a single supplication, along with SHA-512,

of an init() function that prepares the eight 64-bit variables; h0, h1, h2, h3, h4, h5, h6 and h7 [51]. This is followed by a series of invocations of an _update() function and a finalise() function. SHA-256 tends to allow more security and protection than other hashing algorithms and is used and trusted by prominent technology and public-sector agencies. Moreover, since there are 2256 different possible hash values in SHA-256, it is highly unlikely that two different documents will have the same hash value. It is also exceptionally easy to calculate and generate a hash using this system, and both small and large files take the same amount of time to generate. As SHA-256 is deterministic, this suggests that it is incredibly easy to determine the authenticity of a file, as a specific file input will always produce the same hash number. It is therefore impossible to alter a file without in turn altering the hash number, which leaves digital evidence behind and is known as the avalanche effect. Avalanche effect In cryptography, the avalanche effect is the desirable property of cryptographic algorithms, typically block ciphers and cryptographic hash functions, wherein if an input is changed slightly (for example, flipping a single bit), the output changes significantly (e.g., half the output bits flip) [51][51]. The principal reason that leaders in technology use SHA-256 though, is because it has not been, in essence, broken, like many other prevalent hashing algorithms.

6.3 Users' Interactions with the System

We designed the system to be easy to use, allowing users to login with the frontend function and then access and distribute their documents if they so choose; Figure 6.5 shows the system home page where users can access the system. Users' documents are uploaded on the blockchain via the smart contract, with documents also being uploaded by the university for verifiable purposes. As students can access their uploaded documents, they can send them to potential employers, while employers can also verify the document using the document hash to search the system.

6.3.1 Admin Interaction with the System

To begin, admins must log in to the system using the correct login credentials previously supplied to them before being forwarded to the admin dashboard, wherein the menus are laid out. Admins can choose from 'Add University', 'University Manage', or 'Student Manage'. The 'Add University' tab allows admins to add a university into the university database by completing the form. Later, if necessary, the 'University Manage' tab allows admins to edit and delete universities.

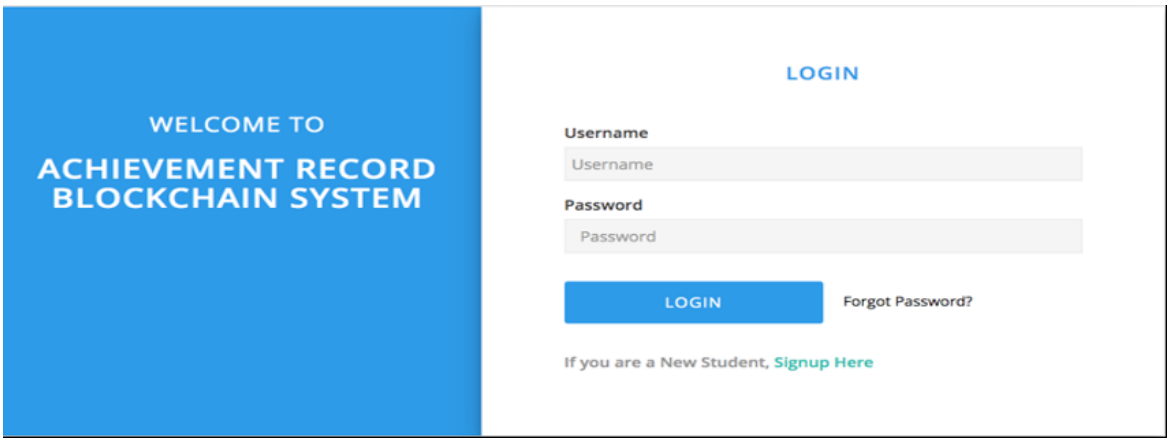


Fig. 6.5 System Homepage

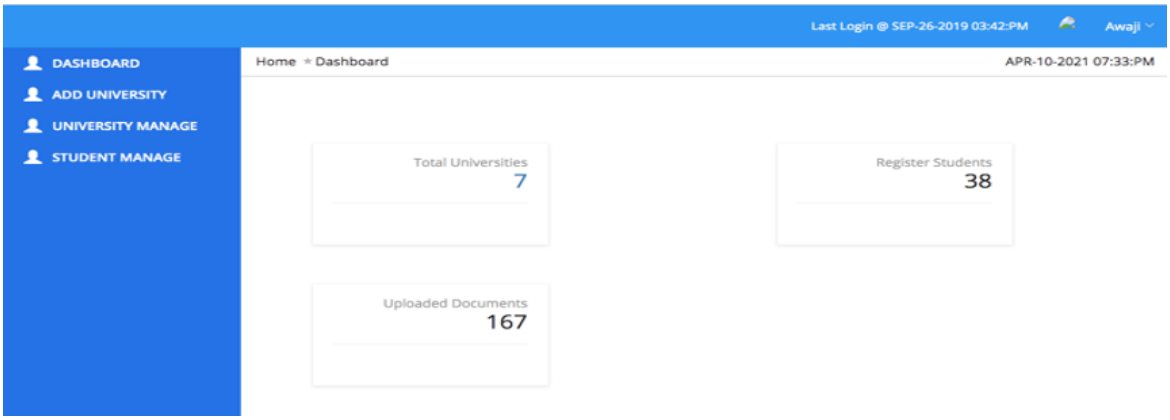


Fig. 6.6 Admin Dashboard

6.3.2 University Interaction with the System

The university user must log into the system, again with correctly supplied credentials, and then will be taken to the university dashboard; as showed in Figure 6.7. The user will be presented with specific menus, including 'Document List', 'Upload Document', 'Add Students' and 'Manage Students'. By clicking on 'Document List', the university user will be able to view a list of the students' documents and clicking on any specific document will produce information about the relevant student. The 'Upload Document' tab allows the user to upload a student's document by entering their details. If the document type is already available in the system, they can upload the document straight away. If not, they must first add the specific document type. The 'Add Student' tab enables the user to add a new student and all of their relevant details into the database, whereas the 'Manage Students' tab allows the university user to see a complete list of students, editing where necessary.

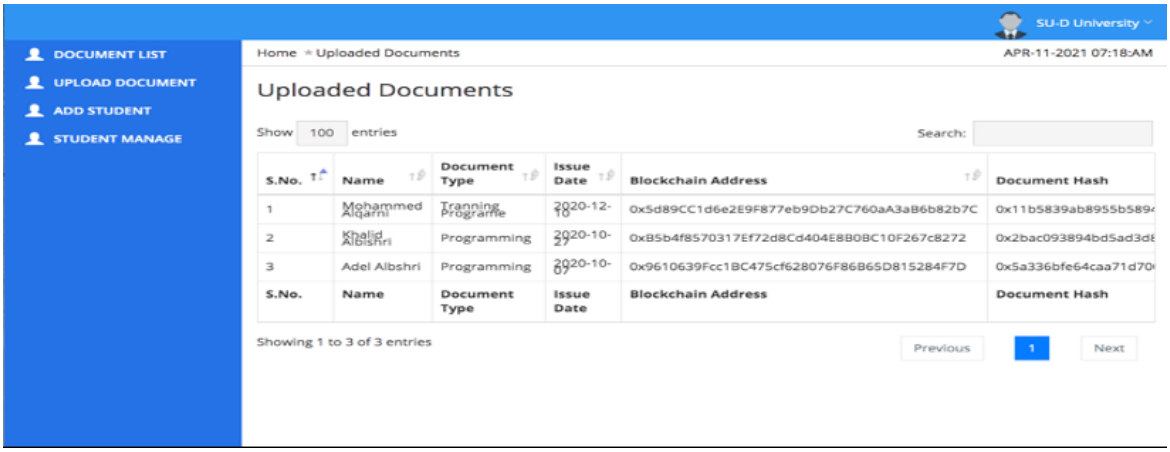


Fig. 6.7 University Dashboard

6.3.3 Student Interaction with the System

The student homepage in Figure 6.8 allows university students to register themselves in the system. They are provided with a unique user ID and password, and, once entered correctly, will be redirected to the dashboard. If they enter their details incorrectly, an error message will be displayed. They will stay on the login page until they enter the correct details. Once successfully logged in, students can see their information on the dashboard and are also presented with a list of certificates that have been uploaded by universities. Using the email system, students can share their documents with different employers, who will receive a link directing them to a document verification page.

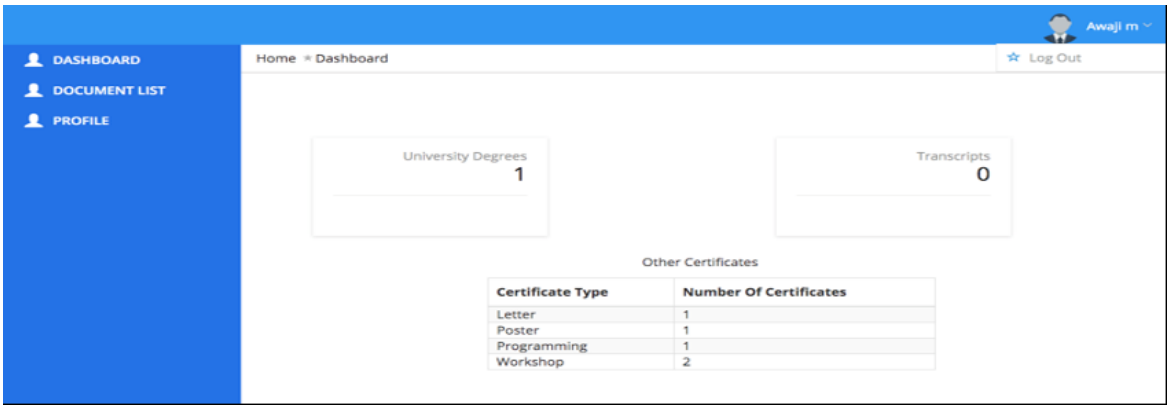


Fig. 6.8 Student Dashboard

6.4 Conclusion

In conclusion, the primary objective is to provide guidance on developing the proposed system using the design mentioned in (chapter 5). Additionally, this chapter discusses the end-user interface with the system. Finally, we describe the implementation of each component and justify our pick. The frontend (centralised layer) was implemented with HTML, CSS, JS, web3, Jnode, in addition to a SQL database for data storage. At the same time, the backend (decentralised layer) was implemented by writing the smart contract in Solidity [126] and then sending it to the Ethereum blockchain. We verified the frontend of the system by testing each function separately to ensure the output was correct and free of bugs and errors. The smart contract verification in the backend is completed using the online Remix IDE [72], where we can run the smart contract in the blockchain testnet. Then we released the system and designed an experiment for end-users to utilise the system in order to collect data for the evaluation task. Therefore, we discuss the experimental and evaluation details in chapter 7, in order to collect data for evaluation purposes, we discussed an experiment to enable end-users to employ the proposed system and then evaluate it through a number of evaluation methods.

Chapter 7

Evaluation

Overview

We mainly aim in this research to provide the stakeholders with a system that is user-friendly and trusted. Therefore, in this chapter, we first evaluate the system usability utilising the System Usability Scale (SUS) test [23]. Then, we adopt the End User Computing Satisfaction (ECUS) test [65] to evaluate the feasibility of the system. Furthermore, to understand if our proposed system is a motivating solution for users to improve their skills and enhance their learning future, we designed a mixed-methods questionnaire to collect and analyse data so as to evaluate this objective. We collected data by way of an experiment which entails the end-users using the system then analyse their reflections from the answers to the questionnaire. Likewise, we analysed the system's feasibility in terms of cost and transaction confirmation time.

7.1 Contribution

The main contribution of this chapter is as follow:

1. Conducting an extensive analysis of the system usability by adopting the System Usability Scale (SUS) method.
2. Conducting an extensive analysis of the satisfaction of system users by adopting the End-User Computing Satisfaction (EUCS) method.
3. Conducting an extensive analysis of assessing system capability to affect the system's users positively in terms of the aim of learning, planning for future learning, employment and providing proof of skills.

4. Conducting an extensive analysis of two variables, First, the delay time represents the transaction confirmation time. It refers to the time a transaction takes from its broadcast to the blockchain and addition to the distributed ledger. Second, the cost of the transactions; the cost represents the mining fee (Gas). Gas refers to the unit that measures the computational effort required to execute specific operations on the Ethereum network.

7.2 Experiment: End-users Using the System

To appraise our solution, we designed an experiment to collect data from the end-users of the proposed system through different evaluation methods. Figure 7.1 illustrates the stages of the experiment.

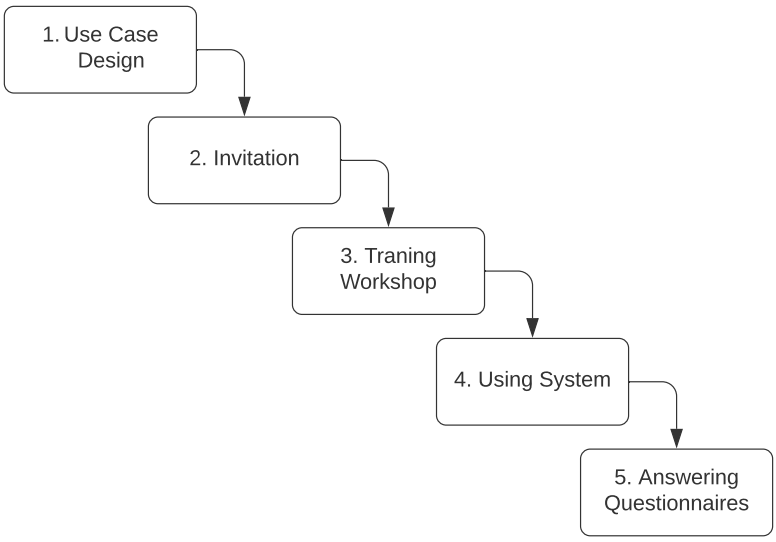


Fig. 7.1 Experiment Steps

Step 1: Experiment Use case

The use case is for the participants to be able to use the system. The participants consist of two types of users: university and student. First, participants can practice their tasks based on their type. Then they answer the questionnaires. Once we receive the answers, we do an intensive analysis of their responses to evaluate the system.

Step 2: Invitation

The literature on web survey explains that the design of mail invitations or advance letters can affect response rates in both surveys and interviews [71]. To tackle this issue, we designed two invitations to invite the universities or educational institutions. The other invitation we created was the students' invitation. Both invitations were intended to be short and clear and provide the potential participants with all the information they may need to participate (see Appendix C,1&2 for the invitation forms). In total, we received responses from six universities as shown in Table 7.1; 30 students from those universities agreed to participate in our evaluation of the proposed system.

Table 7.1 Evaluation Participants' Details.

Participant	Geographical Location	Educational Background of Participants
U1	Saudi Arabia	non-computing
U2	Saudi Arabia	non-computing
U3	Saudi Arabia	non-computing
U4	UK	non-computing
U5	UK	non-computing
U6	USA	non-computing

Step 3: Training Workshop

This step aims to give the participants, who agreed to participate in the evaluation process, practical training regarding using the system and answering their questions. In this step, we also designed an infographic that clearly explained to participants the steps required to use the system (see Appendix C,3 for the infographic).

Step 4: Using System

In this step, participants will start using the system based on their type of access, "university or student". Then, the participants will apply the use cases that we explained in Chapter 5, page 83 relevant to their responsibilities within the system.

Step 5: Answering Questionnaires

Finally, in this step, participants will receive links to the questionnaires that we designed for evaluation purposes via their email. The following sections present the questionnaires details and their results.

7.3 System Usability Scale (SUS)

To appraise our solution's usability, we will undertake a System Usability Scale (SUS) test explained in Chapter 2, Section 2.6.1.

7.3.1 Reliability

As a result of the statistical data, the reliability of the variables intends to measure the overall consistency under different conditions. Thus, the value of Cronbach's Alpha needs to consider how the internal consistency can be measured. Typically, the standard value to measure reliability is greater than 0.5 [91]. This indicates the variables' accepted level. However, a value greater than 0.8 indicates strong reliability.

Data Interpretation:

In the current case, Cronbach's Alpha value is 0.771 as shown in Table 7.2, indicating strong reliability since the value is greater than 0.5. It can also be said that the estimated value greater than 0.77 indicates the good reliability, reflecting the strong interrelation between all variables.

Table 7.2 Reliability Statistics SUS Test

Cronbach's Alpha	N of Items
0.771	10

7.3.2 Results

The systems usability scale (SUS) is the scale that assesses the usability of a system through ten different questions regarding the effectiveness of a system. The survey was conducted with 30 participants who stated their experience with the SUS. The participants were the students of universities of different countries. The test was conducted to primarily assess the usability of the proposed system as to whether the objective of building the system has been achieved. The respondents were asked to answer the ten questions associated with the usability of the system in which they had to answer on a scale from strongly agree to strongly disagree. The Likert scale was used to gather the responses of participants in relation to the usability of the system. The correct process including a few steps was followed to determine the most repetitive response from strongly disagree to strongly agree to conclude. In the table 7.3, n is the number of participants who checked that response, while the second

column shows the average number of answers for 1, i.e. strongly disagree and so on. The weighted average column represents the weighted average value of all the five responses. This shows that if the value is close to 5, most of the participants strongly agree and if it is close to 1, it means most of them disagree. When asked if they thought they would like to use the system more often, 36.67% and 40% agreed to the statement indicating that they were interested using it. When asked if the system was complex, 43.33% of participants strongly disagreed and 30% disagreed,indicating that the system was easy for them to use. It has also been established that most of the participants believed that the system would be easy to use. They were then asked if they would need the support of a technical person. It was found that they do not think that they would need any kind of support while using this system, as 30% and 43.33% disagreed and strongly disagreed with the statement. They disagreed with the question that there was inconsistency in the system and agreed with the statement that people can learn using this system quickly. It should be mentioned that 63.33% strongly disagreed and 23.33% disagreed with the statement that the system is burdensome to use and that they were also confident about using the system. Participants also disagreed with the statement that they had to learn a lot of things before using this system. The overall analysis suggested that participants found the system helpful and easy to use; they believed that there was no need for any additional learning and neither does the system require any expertise to be used. Participants found the system user-friendly and extremely useful which indicates that participants were happy about using this system.

Table 7.3 Results of the SUS Questionnaire Based on the Participant's Answers.

	1 Strongly Disagree		2		3		4		5 Strongly Agree			
Q	Avg	n	Avg	n	Avg	n	Avg	n	Avg	n	Total	Weighted Average
1	0.00%	0	0.00%	0	23.33%	7	36.67%	11	40.00%	12	30	4.17
2	43.33%	13	30.00%	9	13.33%	4	3.33%	1	10.00%	3	30	2.07
3	0.00%	0	0.00%	0	3.33%	1	33.33%	10	63.33%	19	30	4.6
4	30.00%	9	43.33%	13	10.00%	3	6.67%	2	10.00%	3	30	2.23
5	0.00%	0	0.00%	0	13.33%	4	36.67%	11	50.00%	15	30	4.37
6	40.00%	12	36.67%	11	10.00%	3	0.00%	0	13.33%	4	30	2.1
7	0.00%	0	0.00%	0	16.67%	5	30.00%	9	53.33%	16	30	4.37
8	63.33%	19	23.33%	7	0.00%	0	0.00%	0	13.33%	4	30	1.77
9	0.00%	0	6.67%	2	6.67%	2	40.00%	12	46.67%	14	30	4.27
10	16.67%	5	30.00%	9	26.67%	8	13.33%	4	13.33%	4	30	2.77

The overall results show that the participants are satisfied with the usability of the system and find it user-friendly (figure 7.2.)

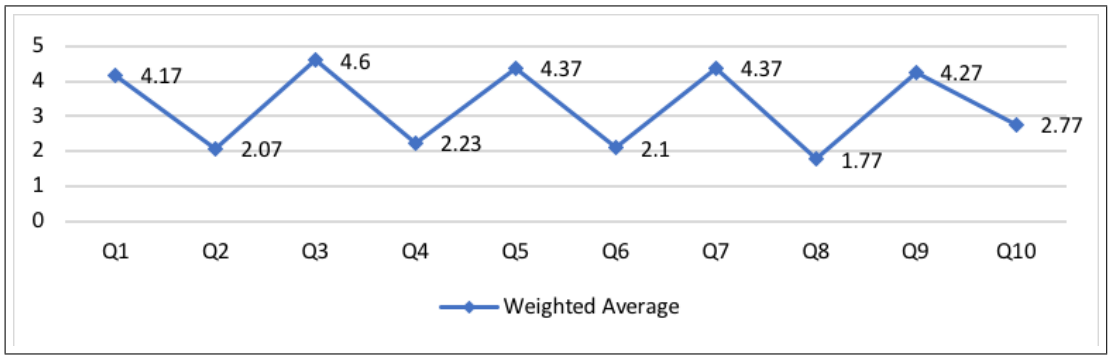


Fig. 7.2 Weighted Average of All Questions.

7.3.3 Discussion

The effectiveness of a system is usually assessed by the feedback of its users as to whether the system assisted them, how easy the system was to use and how much time and effort did the system take to understand. It was determined that the system was extremely useful in terms of ease of use, denoting that the participants believed they would like to use the system regularly. Consequently, 36.67% and 40% stated that they would like to use the system more frequently. Moreover, 43.33% of the participants strongly disagreed and 30% disagreed when asked if the system was complex. It was also established that they do not feel dependent upon anyone to use the system, i.e. no expertise is required to use the system, demonstrating that the system is extremely user-friendly. This feature is considered one of the most important considerations to declare a system effective and usable, 30% and 43.33% disagreed and strongly disagreed with the statement that the system requires some expertise to use. The participants' responses stated that they are satisfied with the usability and efficiency of the system, while it was also ascertained that the system can be learned very quickly without any training or expert support. Neither is the system found to be cumbersome, with the participants feeling very confident while using the system. Overall, the participants stated that they did not face any difficulties while using the system as it does not require any expertise or training. Hence, anybody can easily learn how to use the system.

As in figure 7.3, the grades are presented in the five letters A, B, C, D, and F. Each of the letters covers a range of scores on the scale, as well as the adjectives that are also classified into six categories starting from the Worst Imaginations and ending with Best Imaginations. Regarding the acceptability, if the sus score is between 0 and 50, then the system is considered "Not Acceptable", and it is considered "Marginal" if the sus score is between 51 to 70. On the other hand, a sus score above 71 is regarded as an "Acceptable". Finally, the Net Promoter Score NPS is classified into three categories Detractor, Passive and Promoter. Detractor if the sus score is between 0 to 60, Passive if the sus score is between 61

to 80, Promoter if the sus score is above 81. Over all, figure 7.3 shows a score of 77.1 which falls under good and excellent in relation to rating the system. This denotes a grade B which is a positive indication and rating based on the SUS Score Interpretation.

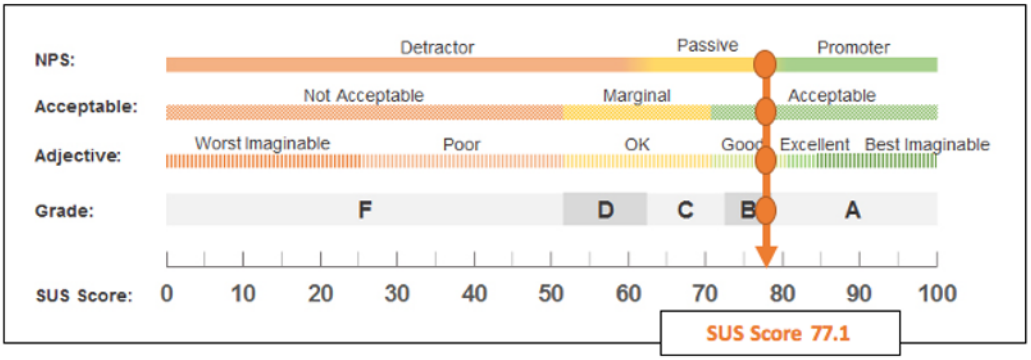


Fig. 7.3 The SUS Score Obtained.

7.4 End-User Computing Satisfaction (EUCS)

To appraise the end-user computing satisfaction, we used the End-User Computing Satisfaction test explained in Chapter 2, Section 2.6.1.

7.4.1 Reliability Test

As a result of the statistical data, the reliability of the variables intends to measure the overall consistency under different conditions. Thus, the value of Cronbach's Alpha needs to consider how the internal consistency can be measured. Typically, the standard value to measure reliability is greater than 0.5 [91]. This indicates the variables' accepted level. However, a value greater than 0.9 indicates strong reliability.

Data Interpretation:

The Cronbach's Alpha value is 0.972 as shown in Table 7.4, indicating strong reliability since the value is greater than 0.9. It can also be said that the estimated value greater than 0.97 indicates the best reliability, reflecting the strong interrelation between all variables.

Table 7.4 Reliability Statistics (EUCS) Test.

Cronbach's Alpha	N of Items
0.972	18

7.4.2 Results

Content

The result has been attained by examining all variables relating to the End-user computing satisfaction test (EUCS) [38]. As per the result indicated by Figure 7.4, it has been determined that the content of the system or application is significant since the majority of users prefer to have precise and sufficient information to gain a better understanding. According to the result, it can be seen that the content of the system is meeting the needs of the participants based on the answers. Moreover, the responses' average weight showed that not all systems offer relevant output as expected by the users. However, it has been claimed that the system's information content successfully meets the users' needs. Furthermore, the collected responses demonstrated that approximately half of the respondents believed that the system offers sufficient information. In this way, the need to improve the system's content has been highlighted as this might help increase the users' end-user satisfaction. Regarding of whether the system offers the exact content necessary, the users showed mixed responses. Thus, it is recommended that some improvement is necessary for the system to ensure end-user satisfaction.

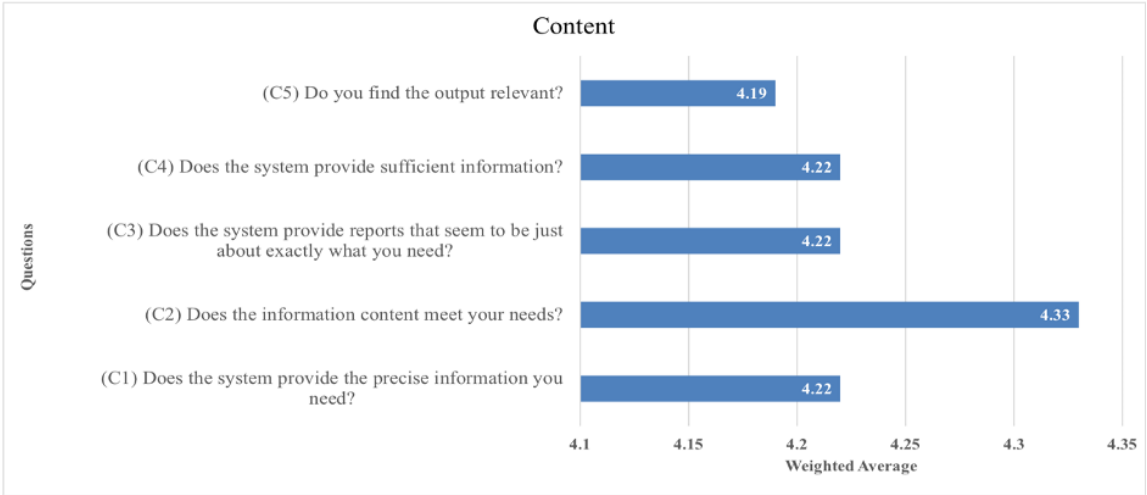


Fig. 7.4 A Set of Questions to Evaluate the Variable 'Content'.

Accuracy

According to the collected data that figure 7.5 illustrates, users shared that most of the system is accurate, which can be an essential factor in increasing users' satisfaction. On examining the graph mentioned below, it can be determined that accuracy has a direct link with the reliability of the output since one of the questions was related to asking about the reliability of the users so that the accuracy level can be determined. As per the collected outcome, it has resulted that an average of 4.3 average of 4.3 of users agreed with the statement that the output from the system is reliable. Based on the reliable result, it can be measured that the system of a specific application is accurate to use. The result also shared that dependency is also related to the accuracy aspect since most users shared that the system is dependable, which means offering an accurate outcome.

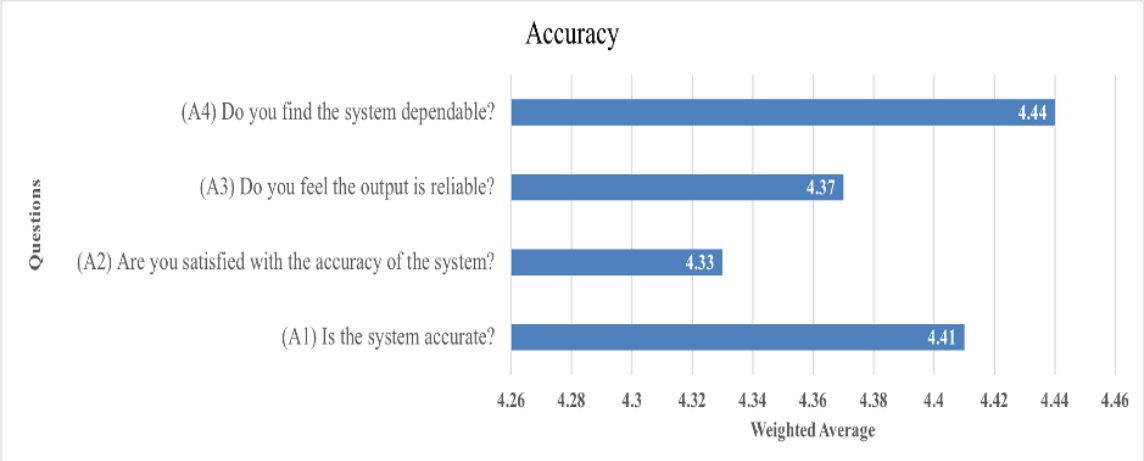


Fig. 7.5 A Set of Questions to Evaluate the Variable 'Accuracy'.

Format

Another variable used to measure the EUCS is the format. Figure 7.6 illustrates the data collected has attained the format of the system or a specific application is based on the usefulness of the output, clearance of the information, understandable layout and easiness. All these factors collectively help make the system accurate as the collected result reflects that roughly 4.5 of users considered it useful information. According to them, a system that presents data in a useful format is more reliable to access. The graph showed that almost 4.3 of users indicated clear information so that this aspect also helps maintain the users' satisfaction level. Regarding the users' happiness rate for the accuracy factor, 4.36 of users are relatively happy. Thus, it has resulted in a comfortable and understandable website layout

that shows the system's reliable format. Another question related to the system's format is about how the user, application or system follows the required format. It should be mentioned that most of the system has an understandable output and thus, is concluded as a formatted one.

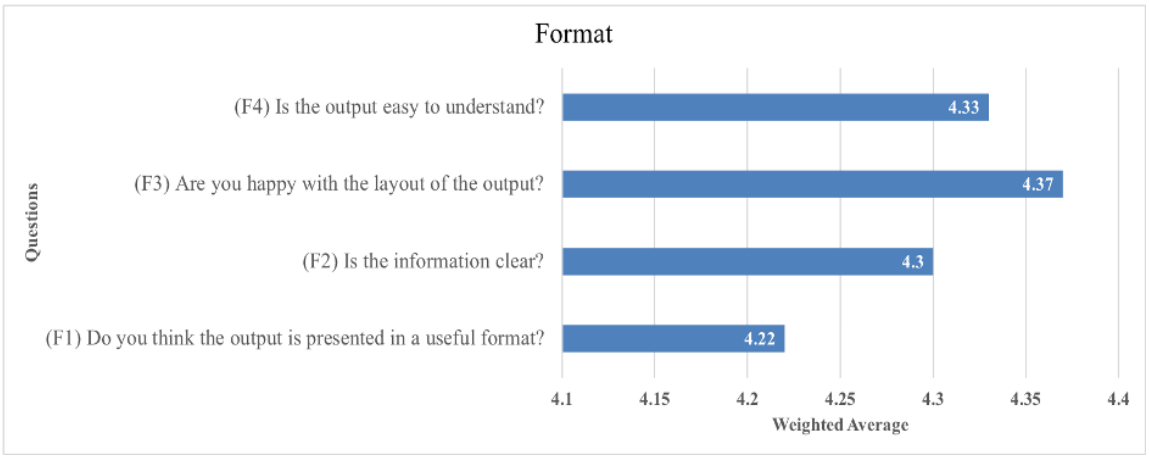


Fig. 7.6 A Set of Questions to Evaluate the Variable 'Format'.

Ease to Use

It is also essential to consider the ease of use to ensure end-user satisfaction. Therefore, some questions were asked related to that aspect. As a result, as Figure 7.7 illustrates, the system is user-friendly since the majority of them shared a positive response related to this question. Through this, it is believed that ease of use of the system or application depends on the user-friendly aspect. However, this is also affected by the system's usability rate. The collected data also revealed that efficiency is one of the factors associated with ease of use as the average weight rate from the end-users is ascertained to be 4.4 approx. Owing to this analysis, it can be said that users may experience ease of use if the system is user-friendly, simple to use and efficient enough to operate as per the needs of the users.

Timeline

With timeliness, the end-user satisfaction rate can be examined since numerous factors ensure satisfaction and usage consistency. Accordingly, it has been found that the majority of users had a good experience with the selected system, as 4.37 of users shared a satisfactory response. Conversely, Figure 7.8 showed that the system does not provide up-to-date information, which might negatively affect the satisfaction rate. On achieving end-user

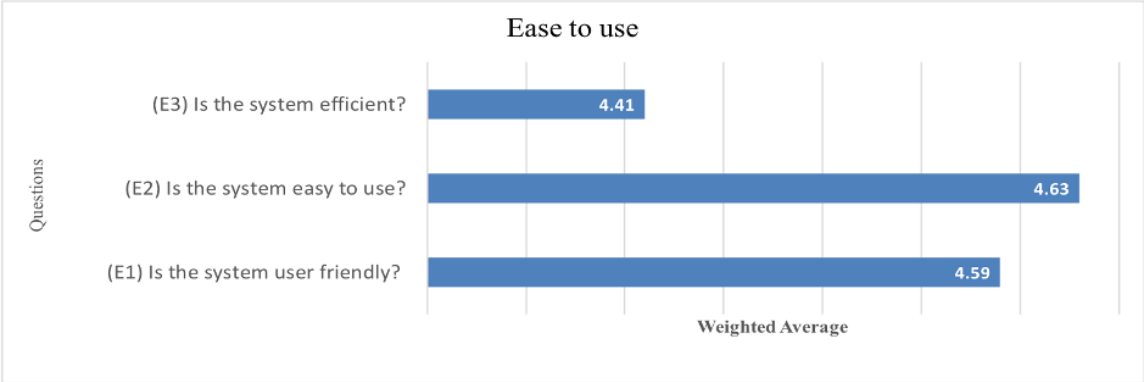


Fig. 7.7 A Set of Questions to Evaluate the Variable 'Ease to Use'.

satisfaction, it was revealed that the system needs to provide up-to-date information since this is an important aspect.

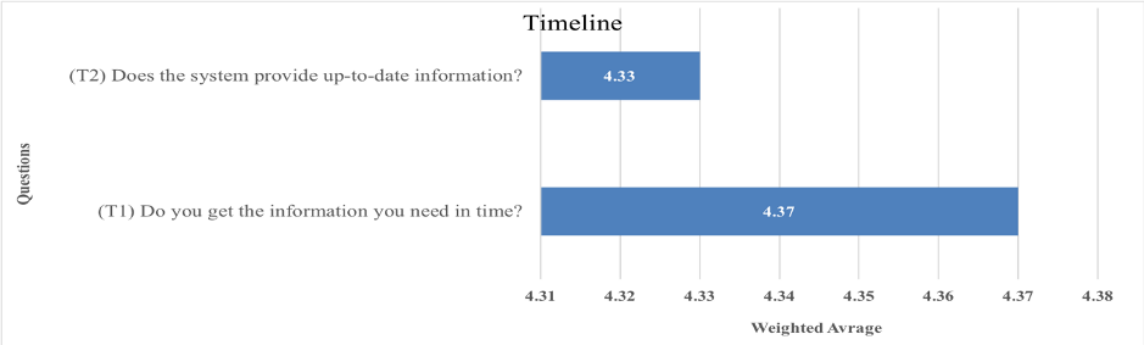


Fig. 7.8 A Set of Questions to Evaluate the Variable 'Timeline'.

7.4.3 Discussion

On conducting the examination of the survey results, it was noted that end-user satisfaction is the method used to measure consumers' satisfaction level with related variables like content, accuracy, format, ease of use and timeliness. The results attained from the users revealed that the system's information needs to be precise as the majority of users show satisfactory responses if the information is precise and well-defined. Not limited to this, it has been determined that content has a significant relationship with end-user computing satisfaction since the information is the main feature that helps to meet the needs of the users. Likewise, it has been evaluated that users, preferably searching for a system or application that comprises sufficient information, for instance the users' survey, reflected high preference in relation to this aspect. The collected data asserted that the system needs to provide the exact information that the users require or else this might negatively affect the end-user computing satisfaction.

Concerning another variable, i.e., accuracy, it has been examined that end-user satisfaction also depends on the system's accuracy since the main answers collected from the end-users reflect the system's accuracy in every aspect. Besides, it has also been found that the current system shared satisfactory accuracy that would contribute to ensuring the satisfaction level of the users. Meanwhile, the importance of format has also been discussed where the system's presentation plays a vital role in increasing users' satisfaction levels. The response collected from the users revealed that clear information also helps to reflect the satisfaction level of end-users as regards the system's format. It has been determined that users are more likely to use the system if it contains user-friendly information and it is easy to use. Furthermore, end-user satisfaction also depends on those who are satisfied with the system sharing information in real time. They also prefer to access the up to date system. Thus, collectively, all variables are contributing to measure and ensure end-user satisfaction. Based on the result, it can be asserted that end-users are satisfied as the proposed system has a high level of satisfaction with its content, format, accuracy, ease of use and timeline.

7.5 Evaluating the Reason for Learning, Employment, Planning and Proof of Skills

We designed a questionnaire to collect data from users to assess the effectiveness of the proposed system in terms of achieving a set of objectives, as shown in Figure 7.10. The total number of students who answered the questionnaire is 30 students from nine different universities, as shown in Figure 7.9 below.

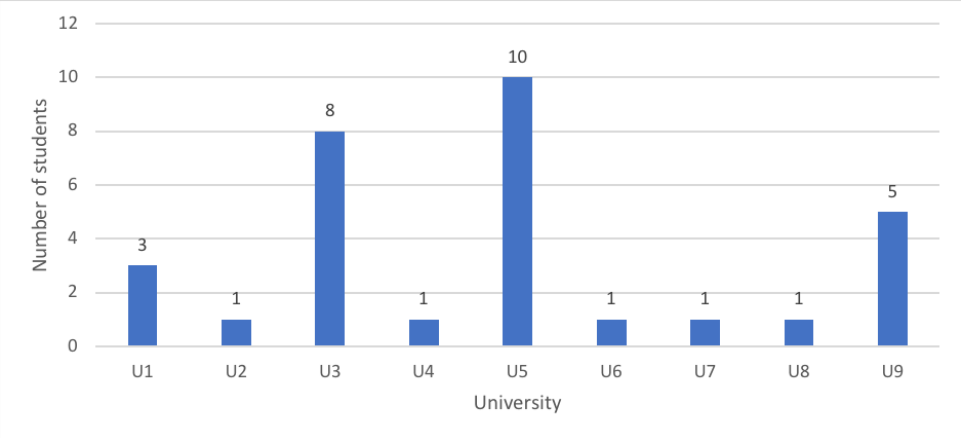


Fig. 7.9 Participants from Students' Type.

7.5.1 Reliability Test

As a result of the statistical data, the value of Cronbach's Alpha needs to consider how the internal consistency can be measured. Typically, the standard value to measure reliability is greater than 0.5 [91]. This indicates the variables' accepted level. However, a value greater than 0.9 indicates strong reliability.

Data Interpretation:

The Cronbach's Alpha value is 0.632 as shown in Table 7.5, indicating strong reliability since the value is greater than 0.6. It can also be said that the estimated value greater than 0.63 indicates the good reliability, reflecting the strong interrelation between all variables.

Table 7.5 Reliability Statistics Reason for Learning, Employment, Planning and Proof of Skills.

Cronbach's Alpha	N of Items
0.632	6

7.5.2 Results and Discussion

Referring to the motivation of learning, employment, planning and proof of skills, a high satisfaction level with the system has been attained given that most respondents agreed with the system's efficiency. On evaluating Figure 7.10, it is established that the system encourages students to learn and improve their skills and earn knowledge from various resources besides the academic courses and modules, as most of the participants, 96.15%, agreed with this point. Similarly, 88.46% of participants answered yes to the question asking if the system helps them build a future learning plan that keeps pace with their future professional aspirations based on what has already been accomplished. Hence, it has been demonstrated that the system helps to demonstrate a learning plan through the participants' answers. Encouragingly, 76.9% of the respondents believe that the system facilitates the hiring process in the future and increases students' connectivity with future employees. Additionally, most participants, 96.15%, agreed that the system provides proof of students' qualifications and skills that are not recorded in their official academic transcripts. Exactly half of the participants did not know that the system contains blockchain and smart contract technology. They did not need to learn blockchain to use the system, as 84.6% of them answered red"No" to the last question shown in Figure 7.10. On evaluating the result, it has been ascertained that participants found the system easy to use and friendly, even though it integrates blockchain technology. As most participants did not know the system has blockchain, this means that we successfully designed a user-friendly interface for the system that prevents users from dealing with blockchain complexity. The collected data reveals that system integrating encourages the students to improve skills and allows them to earn knowledge from multiple resources. In addition to the modules and course learning, students can now increase their learning motivation and enhance their planning skills. The system also contributed to connecting the stakeholder and employees with the students by which the hiring process can be managed efficiently.

Fig. 7.10 Evaluating Motivation of Learning, Employment, Planning and Proof of Skills by Students.

7.6 Transactions Confirmation Time and Cost

This analysis discusses two variables:

- **Delay Time:** Delay time represents the transaction confirmation time. It refers to the time a transaction takes from its broadcast to the blockchain and addition to the distributed ledger.
- **Transaction Cost:** The cost represents the mining fee (Gas). Gas refers to the unit that measures the computational effort required to execute specific operations on the Ethereum network. Gas fees are paid in Ethereum's native currency, Ether (ETH).

The collected data revealed 219 transactions taking approximately 17 minutes and 32 seconds to confirm. The average time to confirm the transaction was 0.24 minutes. The data shown below represents the total transaction fee measured as 00.767 Ether; however, the average transaction fee stood at 0.01097 Ether. On evaluating the transaction fee in USD, the attained rate stood at $657.409. Similar to this, the average transaction fee in USA dollars stood at $6.1574. Thus, the Table 7.6 below shows the overall summary of the transactions discussed in the study.

Table 7.6 Transaction Times and Costs.

Total Number of Transactions	219
Total Confirmation Time (MM: SS)	17:32
Average Confirmation Time (MM: SS)	0.24
Total Transactions Fee (Ether)	0.76703077 Ether
Average Transactions Fee (Ether)	0.01091671 Ether
Total Transactions Fee (USD)	$657.409294
Average Transactions Fee (USD)	$6.15745258

Each transaction has also been calculated using different universities to obtain more comprehensive results. In total, six universities are targeted as shown and explained below. According to the gathered data, university 1's total number of transactions was 45, whereas the confirmation time was 10 minutes 5 seconds. Meanwhile, the average confirmation time was 55 seconds. Accordingly, the transaction fees were 0.21992263 Ether. Conversely, the average transaction fee was 0.00549 Ether. Data from the second university confirmed that 17 transactions took place. Accordingly, the result showed that the total confirmation time was 3 minutes 44 seconds; however, the average confirmation time was 14 seconds. In addition to this, the transaction fee was in Ether, with the average transaction fee being 0.00319 Ether.

Figure 7.11 shows that the average confirmation time for transactions varied per university. For instance, university 1 had an average confirmation time of 0.01 minutes. University 2 measured 0.009 seconds, while university 3 had the highest average transaction confirmation time with a rate of 0.091 seconds. The confirmation time for university 4 reached 0.025 seconds. The average time for university 5 stood at 0.005 seconds. However, this shifted to a confirmation time of 0.01. Universities 1 and 6 took the same time, whereas universities 4 and 5 had varying times. University 3 took the most time with 0.091 seconds.

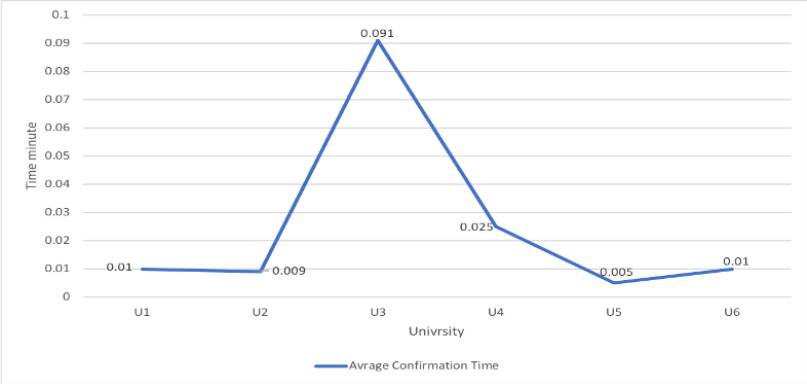


Fig. 7.11 Average Confirmation Time for Transactions.

Figure 7.12 illustrates the number of transactions while comparing them with an average confirmation time. University 1 had 45 transactions. University 2 had 17 transactions, whereas university 3 had 18. University 4 handled 30 transactions. Additionally, universities 5 and 6 had 28 and 8 transactions, respectively. Universities 1 and 6 took the same time. University 1 completed 45 transactions, whereas university 6 managed only 8. The assessment not only depends on the time spent but also the number of transactions. The difference is significant. University 2 took 0.009 seconds and performed 17 transactions, university 3 carried out 18 transactions in 0.091 seconds, university 4 conducted 30 transactions in 0.025 seconds and university 5 carried out 28 transactions in 0.005 seconds. The highest number of transactions was by university 1 with 45 undertaken in the least amount of time by any of the universities.

Figure 7.13 shows the total cost of the transactions in dollars. The findings showed that university 1 had a cost of $125.25; however, university 2 had a cost of $33.23. In addition to this, university 3 had a cost of $25.65. Meanwhile, university 4 had 67.59% of the cost. According to the graph below, the transaction costs of universities 5 and 6 stood at $35.92 and $0.068, respectively. The transaction cost for university 1 was $125.25, for university 2 it was $33.23, for university 3 it was $25.65, for university 4 it was $67.49, for university 5 it was $35.92 and for university 6 it was $0.068. The highest transaction cost was university 1

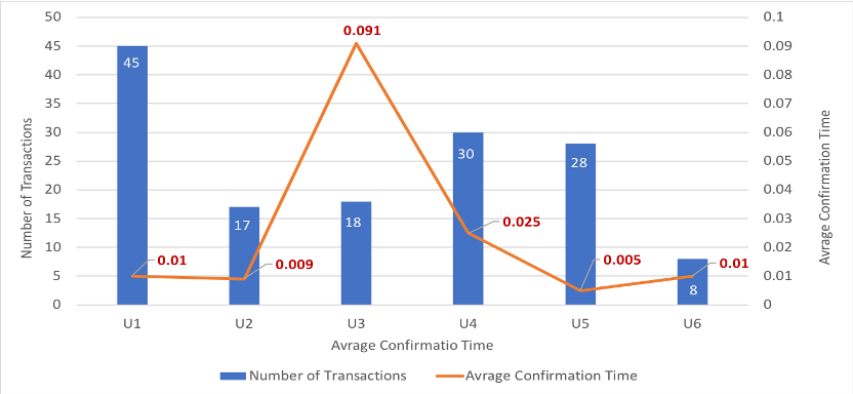


Fig. 7.12 Number of Transactions and Average Confirmation Time

and the lowest was university 6. University 1 performed the most transactions, meaning the costs remain high. The transaction chart shows the cost variation among the universities.

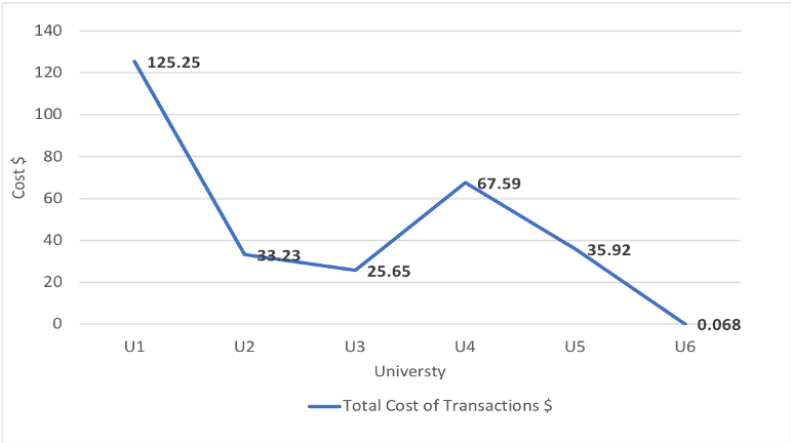


Fig. 7.13 Total Cost of Transactions in US Dollars.

The average transaction cost, measured in US dollars, varied according to the university, as shown in Figure 7.14. Consequently, university 1 had the highest average transaction cost. Apart from this, the final product indicated that university 6 had the lowest average transaction cost, with a rate of $0.007. Meanwhile, all other universities had respective average transaction costs. The average transaction cost for university 1 stood at $3.13 and for university 6, the figure was 0.007. Thus, university 1 had the highest transaction cost, whereas university 6 demonstrated the lowest. Additionally, university 1 carried out 45 transactions, meaning the average cost proved higher than the other universities. University 1 undertook the most transactions in the least time. For instance, university 2 had a cost of $2.07, university 3 had a cost of $1.51, university 4 had a cost of $2.25 and university 5 had an average transaction cost of $1.38.

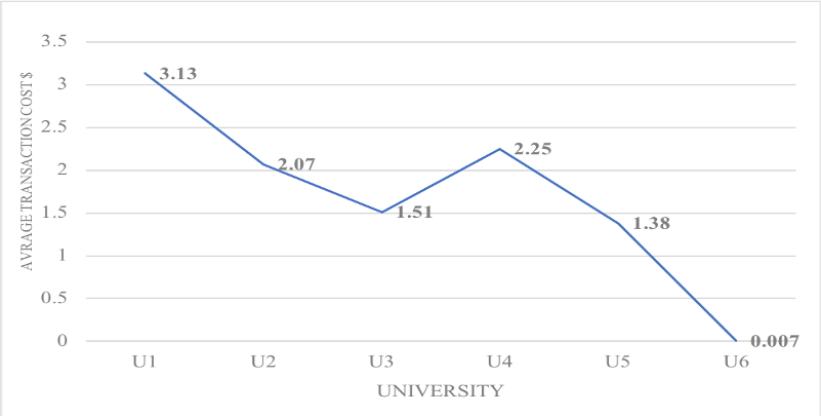


Fig. 7.14 Average Transaction Cost US Dollar.

Conversely, the study found that all universities deal with different transaction costs (Ether), as shown in Figure 7.15. University 1 had the highest such costs with a rate of 0.219 Ether, whereas university 2 had the lowest with a rate of 0.051 Ether. The total cost of transactions was measured as 0.114 Ether, obtained from university 4. Meanwhile, university 3 had a transaction cost of 0.05 Ether.

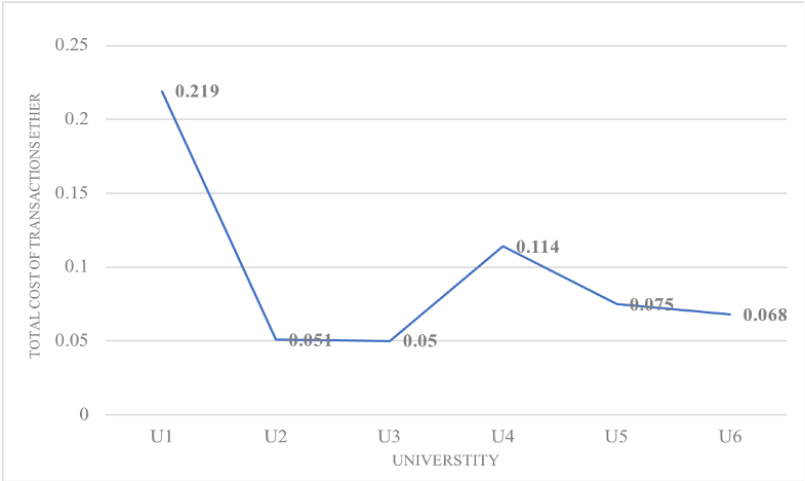


Fig. 7.15 Total Cost of Transactions (Ether).

The data analysis compared the number of transactions and total cost (Ether). The findings as Figure 7.16 illustrates; show that university 1 had the highest number of transactions while dealing with costs of 0.219 Ether. The number of transactions resulting from university 2 stood at 17; however, its total cost reached 0.051 Ether. Similarly, the total transaction cost for university 4 was 0.114 Ether, whereas the number of transactions stood at 30. The cost of Ether varies according to the number of transactions, with university 1 having the most Ether and university 3 the least. Although universities 3 and 6 had approximately the same

Ether costs, the number of transactions were different. For instance, university 3 made 18 transactions, whereas university 6 carried out 8. University 2 made 17 transactions in 0.051 seconds; in terms of Ether cost, university 6 performed the lowest transactions.

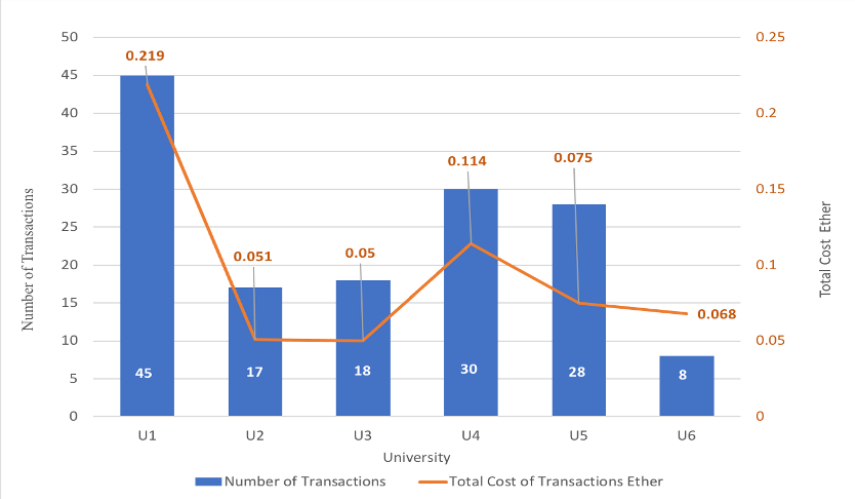


Fig. 7.16 Number of Transactions and Total Cost (Ether).

Figure 7.17 compares the number of transactions and average cost. Consequently, the lowest ratio was associated with university 6, which had 8 transactions. However, the total cost of transactions in US dollars was measured at $0.068. All universities had different amounts of transactions and average costs, as displayed in the graph below. The number of transactions at university 1 stood at 45 and the total cost generated by the university was $125.25.

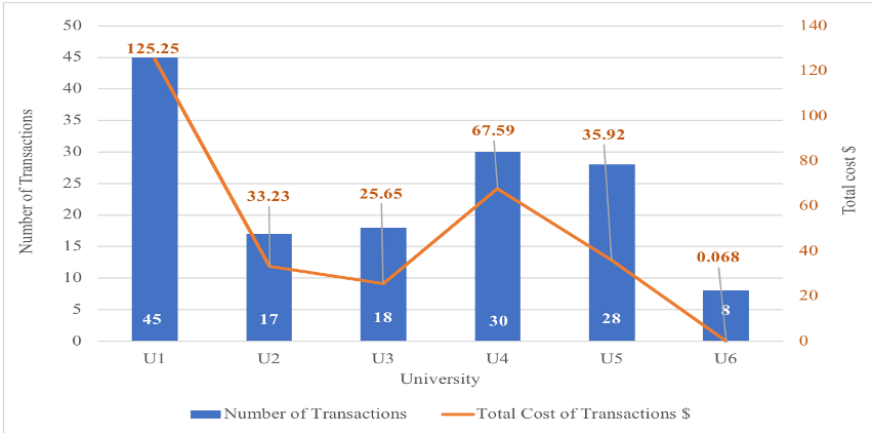


Fig. 7.17 Number of Transactions and Total Cost US Dollar.

This figure represents the highest transaction cost generated by the universities. The cost is high because the university made the highest number of transactions in the least time. The

lowest transactions, 8, were made by university 6, and the cost was low, with a figure of 0.068, because the institution made the fewest transactions at the same time as university 1. Here, the study determines that both the time and amount of transactions in a certain time count when generating costs.

7.6.1 Discussion

This findings obtained by this research show different average transaction confirmation times on blockchain for each university. In the same context, the study notes a difference in the cost of transactions for each transaction on the blockchain. Therefore, cost and time to confirm the transaction represent the variables taken into account for the discussion.

Delay Time:

Delay time represents the transaction confirmation time. In particular, the time that a transaction takes from its broadcast to the blockchain is added to the distributed ledger. From the quantitative data analysis in the previous section, the findings indicate that for 219 transactions, there exists a fluctuation in the average transaction confirmation time between the universities. Ethereum network congestion might represent the cause of delay in the transaction. In terms of transaction confirmation times, the analysis demonstrates that among the universities, the average confirmation time proved different, as shown in Table 7.6. This situation indicates that the variations in transaction time can evaluate the system's efficiency when added to the blockchain. Figure 7.12 demonstrates the average confirmation time and number of transactions handled by each university. By considering the output provided in the previous section, the study ascertained that the number of transactions handled by university 3 was only 18, although it took 0.09 minutes on average to complete the transaction. Meanwhile, the figures reveal that university 3 had the most transactions, but it took only 0.01 minutes on average for the transaction to be confirmed. Hence, the average confirmation time does not depend upon the number of transactions handled by the system but the efficiency of the blockchain system and congestion on the Ethereum blockchain. When a blockchain network experiences peak traffic, it delays transactions. Other factors may also delay transaction confirmation, such as the gas limit. Proportionality exists between the gas limit determined by the sender and the blockchain mining process. Gas prices are denoted in Gwei, which itself is a denomination of Ether. Transactions with higher gas limits attract miners and therefore, operations with a lower gas limit value will continue waiting.

Transaction Cost:

The cost is the mining fee, 'Gas', which refers to the unit that measures the computational effort required to execute specific operations on the Ethereum network. The purpose of gas is to control the resources that a transaction can use since it will be processed on computers worldwide. Gas is separate from ETH so as to protect the system from volatility in the ETH value and manage the ratios between the costs of various resources that gas pays for, such as computation, memory and storage. Gas also rewards the miners for the work they do. The gas price component of a transaction allows a user to set the price they want to pay in exchange for gas; the price is measured in Gwei per gas unit. Wallets can change the gas price to achieve faster confirmations of transactions. The greater the gas price, the quicker the transaction confirmation. Accordingly, the gas limit for the transactions sent from the proposed system stood at 40,000 Gwei (0.004 ETH). In terms of the volume of data sent in each transaction, this value proves attractive to miners. Consequently, all transactions sent by users during the system evaluation required confirmation in a good average time, as shown in the figures. Lower priority transactions can use a lower gas price which means slower confirmation. The market decides the relationship between the price of ETH and the cost of computing operations in terms of gas. The gas cost acts as a measure of computation and storage used in the EVM, where the gas has a price measured in Ether. When sending a transaction, people can specify the gas price they want to pay in ETH for each unit of gas. This equation calculates the transaction fee:

$$Transaction fee = total\ gas\ used \times gas\ price\ paid\ (in\ Ether) \tag{1}$$

This study can explain why each transaction fee differs and as shown, both factors in the equation play a role in determining the cost of transitions.

- **Total gas used:** the gas limit has been specified in the system for each transaction at the value of 40,000 Gwei (0.004 ETH) to speed up the mining process. It remains unnecessary to use the specified gas limit since transactions must pay for the computational, bandwidth and storage space they consume in proportion to these gas costs. Although a transaction includes a limit, any gas not used in a transaction reverts to the user. In this sense, the value of 'total gas used' changes with each transaction and, therefore, the fee changes accordingly.

- **Gas price paid (in Ether):** gas fees are paid in Ethereum's native currency (ETH). Gas prices are denoted in Gwei. A Gwei or Gigawei is defined as 1,000,000,000 Wei, the smallest base unit of Ether. One Gwei equals 0.000000001 or 10^{-9} ETH. Conversely,

1 ETH represents 1 billion Gwei. Consequently, each cost in Ether is different due to the constant change in the value of Ether on the stock market. For example, when this study started the system evaluation process in May 2020, the price of Ether began at \$213.61, meaning that the transaction fee was $0.004 \times 213.61 = \$0.854$. Meanwhile, the transaction fee in February 2021 was $0.004 \times 2036.55.61 = \$8.1462$. This study also noted the significant difference between the cost in less than a year, with the price of Ether more than tripling. Thus, the transaction cost doubled in proportion to the rise of Ether in the price of cryptocurrencies in the stock market. Figure 7.18 shows the change in the price of Ether from May 2020 to February 2021, source[1].

Fig. 7.18 ETH Price from May 2020 until March 2021.

Considering this aspect and the information provided in the previous section, it remains difficult determining accurate confirmation times when sending a transaction from one node to another and adding it to the distributed ledger on the blockchain. Furthermore, the transaction fee remains unfixed and cannot be determined until confirmation of the transaction. Such a situation depends on different factors, as explained in this section. Based on previous findings and the points discussed in this section, the inconstant transaction time depends primarily on the efficiency of the network but remains within the acceptable range. However, this area represents one of the limitations requiring evaluation in future research. The unfixed transaction cost changes depending on the crypto prices on the stock market. This situation may affect the sustainable use of the system. When the cost proves too high, the system will lose its attractiveness to users. Thus, transaction fees represent another significant restriction concerning the system. Despite the effectiveness in other regards and its achievement of research objectives, the material and cost are negative aspects that open the door for future research. To address the issue of transaction cost, some details are important for future researchers to consider. In such a system, we have to execute various functions on

[1] https://www.coindesk.com/price/ethereum.

the blockchain, making the smart contract an essential component in the system structure. Therefore, the blockchain platforms that do not support smart contracts are ineffective in tackling this issue.

Table 7.7 Blockchain Platforms Support Smart Contract.

Platform	**Network Permission**	**Smart Contract Support**
Bitcoin	Permissionless	×
Ethereum	Permissionless	√
Zcash	Permissionless	×
Litecoin	Permissionless	×
Dash	Permissionless	×
Peercoin	Permissionless	×
Ripple	Permissionless	×
Monero	Permissionless	×
MultiChain	Permissionled	×
Hyperledger	Permissionled	√

Table 7.7 illustrates different blockchain platforms. Each has different characteristics and design decisions. The blockchain platforms listed in the table above, Ethereum and Hyperledger, are the only platforms designed to support smart contracts. Ethereum is a permissionless blockchain platform designed to support creating and deploying complex smart contracts on blockchains. While Hyperledger is an open-source collaborative project aiming to advance permissioned blockchains, it aims to provide an infrastructure of different modules and tools for developing blockchain platforms. In theory, developers can use Ethereum or Hyperledger to build the distributed application based on the requirements and objectives of the system. However, Integrating the Hyperledger platform instead of the Ethereum platform into such a system is a useful project for future researchers to tackle the transaction cost issue. From another perspective, private Ethereum blockchain24 may be an appropriate solution to the transaction cost. It comes with zero transaction fees and higher scalability and there are no restrictions. However, switching from public to private blockchain requires a range of additions and modifications in the design of distributed applications. Against public blockchain, private blockchain nodes need permission to join a controlled blockchain and read the chain's state. The network, in this case, is fully centralised; only users with permissions can join the network, write or send transactions to the blockchain. Therefore, converting to a private blockchain is another possible solution for future researchers to tackle the issue.

7.6.2 Benchmarking

From the literature review presented in this thesis in Chapter 2, Section 2.1, Table 2.2 verifies that the CVSS system is the sole system to conduct financial analytic transactions, provide an explanation of the transaction cost, while also providing the confirmation time of transactions on the Ethereum blockchain. Therefore, we compared the financial analysis of our system with the CVSS system in Table 7.8.

Table 7.8 Financial Comparison of CVSS and Our System.

	CVSS	**Our System**
Contract Creation Cost	$19	$10.76
Number of Transactions	60	219
Transaction Cost	$0.15	$6.16
Average Transaction Confirmation Time (mm:ss)	00:60	00:24
Total Transactions Confirmations Time (mm:ss)	05:00	17:32

According to the transaction cost principle, the cost of deploying the smart contract on the Ethereum blockchain for the CVSS system is $19, whereas it is $10.76 for our proposed system because of the optimisation we carried out in the smart contract. Accordingly, it only contains those functions that are necessary to be on the blockchain. The number of transactions conducted in our proposed system is three times greater than in the CVSS. This provides a clearer idea of the transaction cost when using the system. Furthermore, we observe that the cost of a single transaction in the CVSS system is $0.15, while no clarification is provided as to whether this number is fixed per transaction or that it is the average cost for 60 transactions sent through the CVSS system. However, we calculated the mean cost for 219 transactions in our system, as a result of these transactions being sent at various times over a period greater than six months, during the system evaluation carried out by end-users. The mean transaction cost for those sent from our proposed system is $6.16. We can explain the rise in cost as being a consequence of the rapid rise in the price of Ether during the system evaluation period carried out by end-users, as explained previously in the evaluation section. Regarding the transaction confirmation time principle, the mean transaction confirmation time in the CVSS system was 60 seconds, whereas the average for our proposed system was 24 seconds, which is deemed acceptable in contrast to the CVSS. The reason for this may be the gas limit or the propagation delay due to Ethereum network congestion. Additionally, the total transaction confirmation time in the CVSS system for 60 transactions was five minutes. Conversely, the total transaction confirmation time in our proposed 219 transaction system was approximately 17 minutes, which is an acceptable number given the total number of transactions. Verification processing does not require

a waiting time for confirmation and approval from the Ethereum Blockchain nodes. The system compares the information stored on the Blockchain with the certificate information provided by users for verification purposes. Consequently, real-time performance of the verification process is possible. In terms of the trusted achievement record system, we proposed utilising Blockchain technology's advantages in order to digitise the certificate to prevent counterfeiting and illegal modification, as well as to build a reliable, trusted, comprehensive and accessible achievement record for students. The system offers greater transparency and ensures the privacy and convenience of all parties involved, enabling them to perform operations accurately, quickly and efficiently in relation to digital certificate management.

7.7 Conclusion

The outcomes of this chapter is the answer of the research questions **"How to validate the proposed design? How can we evaluate usability, feasibility, and users' satisfaction with the system?"**. The overall analysis of the various evaluation methods we conducted on the system indicated that the system usability score was 77.1, which falls under good and excellent to rate the system. It is grade B which is a positive rating based on the SUS Score Interpretation. Furthermore, based on the End-User Computing Satisfaction (EUCS) test results, participants found the system meets the users' needs. They found it easy to use, accurate, the contents are good, and the timeline for operations is acceptable. We evaluated the User Interfaces (UI) and User Exchanges (UX) system through two quantitative studies. Participants found the system user-friendly and highly useful, indicating that they were happy about using this system. 84.6% of participants believed that there is no need for any additional learning to interact with the system, and the system does not require any expertise for learning the interface. Finally, We evaluated the proposed system's transactions cost and delay. The collected data revealed 219 transactions taking approximately 17 minutes and 32 seconds to confirm. The average time to confirm the transaction was 0.24 minutes. The total transaction fee measured as 00.767 Ether, and the average transaction fee stood at 0.01097 Ether. The record of achievements proposed with the use of blockchain technology is comprehensive in tackling widespread fraud. This system is significantly improved compared to legacy systems, being both more user-friendly and more efficient. The blockchain technology method is a solution that effectively integrates into the existent credential verification ecosystem.

Chapter 8

Conclusion and Future Research

Overview

The first section of this chapter introduces a list of the significant contributions of the research. The research conducted in this thesis is then summarised. Then we explore the research limitations and future work.

8.1 Thesis Contribution

The first and most important contribution in this thesis is proposing the Blockchain-Based Trusted Achievement Record System that designed to be easy to use.The proposed system is new, trustworthy system that stakeholders (such as students, employers, and educational institutions) can use to organise and validate achievement certificates and other relevant documents. Following is a list of the contributions to this research:

- A systematic mapping analysis that collects and analyses blockchain technology research in higher education. This systematic mapping review study aims to address this issue by illuminating existing blockchain applications for higher education and highlighting the research challenges associated with implementing blockchain technology. The most important insights we gained from this study are identifying the taxonomy of the blockchain applications in higher education that contains six different areas and also identifying the eight principal challenges that applications include.
- An investigation study of the requirements to build a blockchain-based achievement recording system by collecting valuable data from participants that reflect their

thoughts and opinions concerning building an achievement recording system based on blockchain and smart contract technology. The outcome of this study provides essential information to design a blockchain-based trusted achievement system and define the system components, tools and mechanisms.

- A conceptual model design of a Blockchain-Based Trusted Achievement Record System. The tools, components, mechanisms, scenarios, use cases and data flow are presented, as well as the design validation process and implementation of a Blockchain-Based Trusted Achievement Record System.

- An extensive study to evaluate system usability using the System Usability Scale (SUS) test. The test was conducted to primarily assess the usability of the proposed system as to whether the objective of building the system has been achieved. As a result, the system achieved a SUS score of 77.9, which falls under good and excellent in relation to rating the system.

- An extensive study to evaluate end-users satisfaction examines system users' satisfaction using the End-User Computing Satisfaction (EUCS) test. Participants found the system meets the users' needs. They found it easy to use and accurate, the contents are good, and the timeline for operations is acceptable.

- An extensive analysis study to assess the system's capability to positively impact the system's users in terms of the motivation to learn, planning for future learning, employment, and providing proof of skills. Participants found the system user-friendly and highly useful, indicating that they were happy about using it, that there was no need for any additional learning to interact with the system, and the system did not require any expertise to learn the interface.

- An extensive analysis study of the system performance through two variables, the delay time and the cost of the transactions. Then, surveying study of the related work to benchmark the outcome of our solution with similar solutions in the research area.

The findings and explanation of the contributions provided in this section are summarised in the following section.

8.2 Thesis Summary

This section summarises the work presented in this thesis, highlighting the significant contributions and findings.

8.2.1 Academic Research on Blockchain-Based Application in Higher Education (Chapter 3)

The main purpose of this study is to answer the research questions **"What are the current blockchain applications in higher education? What are their features and limitations?" in Chapter 1, page 5**. This chapter is contributing by identifying and categorising all peer-reviewed research on blockchain applications in higher education. The task is to determine how blockchain technology is currently being used in higher education and identify gaps in those applications for future research. A systematic mapping study was carried out to collect and analyse relevant blockchain technology studies in higher education. The study concentrated on two primary themes. First, it started by looking at cutting-edge blockchain-based applications that have been developed for educational purposes. Second, it outlines the issues and research gaps that can be addressed in future studies. The outcomes of this study guided us to decide on the research topic and the work that we should carry out in this thesis.

8.2.2 Academic Research on Investigating the Requirements for Building a Blockchain-Based Achievement Record System (Chapter 4)

This study was conducted to answer the research questions:**"How to determine the requirements for building a blockchain-based achievement record system?" in Chapter 1, page 5**. This study intends to gather important information on the thoughts and outlooks of stakeholders on an achievement record system that uses blockchain and smart contract technology. The system would allow stakeholders (for example employers) to validate learning records. Two main aims are investigated. The first is to evaluate the suitability of the idea of building a trusted achievement record for learners in higher education and to evaluate potential user knowledge of blockchain technology. This is to ensure that a designed system is usable. The second aim includes an interview conducted with a small group of participants to gather information about the challenges individuals have when creating and reviewing CVs. Overall, 90% of participants agreed that there was a strong need for a trusted achievement record. In addition, 93.64% of respondents stated that they felt it was invaluable to have a system that is usable by all stakeholders. When tackling the second aim, it was determined that a primary challenge is a lack of knowledge of blockchain and its complexity. In addition, from the employers' perspective, there is a lack of trust due to inaccuracies when students describe skills and qualifications in their resumes. From this investigation, we collect data

that guide us to identify the use cases, components and mechanisms that we need to design such a system.

8.2.3 Blockchain-Based Trusted Achievement Record System Framework (Chapter 5)

The primary contribution is to provide a design of a blockchain-based system, which produces a verifiable record of achievements. In this chapter and the chapter 6 next, the following research questions in Chapter 1, page 5 and 6; were answered:

- **How can the documents be verified using blockchain and smart contract technology?**
- **How can each user's (students, educators, etc.) operations and transactions be specified in our proposed solution?**
- **What are the modelling scenarios of the system use cases?**
- **What are the modelling scenarios of the data flow?**

The system was design based on the hybrid software structure model containing centralised and decentralised layers. The centralised layer presents the frontend of the system, while the decentralised layer (blockchain) has been deployed in the backend of the system. We also designed a scenario that demonstrates the user's interaction with the system. The frontend is responsible for displaying web pages on PCs, Tablets and Smartphones and includes components that execute various functions within the system. The system's backend is based on the Ethereum blockchain, a decentralised network of computer nodes that verify and validate data uploaded to the chain. This operation hashes and adds digital data blocks via a cryptographic link to the chain. We validated the system at a design criticism workshop, during which experts and developers from related domains assisted in refining the system's fundamental design.

8.2.4 Blockchain-Based Trusted Achievement Record System Implementation (Chapter 6)

The primary objective is to provide guidance on developing the proposed system using the design mentioned in chapter 5. Additionally, this chapter discusses the end-user interface with the system. Finally, we describe the implementation of each component and justify our choice. The frontend (centralised layer) was implemented with HTML, CSS, JS, web3,

Jnode and a SQL database for data storage. At the same time, the backend (decentralised layer) was implemented by writing the smart contract in Solidity and then deploying it to the Ethereum blockchain. We verified the frontend of the system by testing each function separately to ensure the output was correct and free of bugs and errors. The smart contract verification in the backend is accomplished using the online Remix IDE, where we can run the smart contract in the blockchain testnet, such as Roston. Then we released the system and designed an experiment of using the system by end-users in order to collect data for the evaluation task.

8.2.5 Blockchain-Based Trusted Achievement Record System Evaluation (Chapter 7)

Our primary objective in this research is to provide stockholders with an easy-to-use and trusted system. As a result, we begin this chapter by assessing the system's usability using the System Usability Scale (SUS) test. Then, we analyse the system's practicality using the End User Computing Satisfaction (ECUS) test. Additionally, in order to determine whether our proposed system is a motivating option for users to improve their abilities and advance their learning future, we created a mixed-methods questionnaire to gather and analyse data pertaining to this idea. We collect data through an experiment in which end-users utilise the system and then analyse their observations based on their responses to questionnaires. The outcomes of this chapter is the answer of the research questions **"How to validate the proposed design? How can we evaluate usability, feasibility, and users' satisfaction with the system?"**

The aggregate analysis of the many evaluation methodologies we used to rate the system revealed that the system's usability score was 77.1, which falls between good and exceptional. According to the SUS Score Interpretation, it corresponds to a grade B, indicating a favourable evaluation. According to the System Usability Scale (SUS) study, the system usability score was 77.1, which is in the range of good to exceptional and corresponds to a grade B, a positive assessment based on the SUS Score Interpretation. Additionally, based on the findings of the End-User Computing Satisfaction (EUCS) test, participants determined that the system met their needs. They found it to be simple to use, accurate, with decent material, and an acceptable schedule for operations. Additionally, we examined the system's User Interfaces (UI) and User Exchanges (UX) via two quantitative studies. The system was deemed to be user-friendly and extremely useful by participants, indicating that they were satisfied with their system with it. Furthermore, 84.6% of participants believe that no further learning is required to interact with the system and that the system requires no skill to learn the interface.

Finally, we examined the transaction cost and delay associated with the suggested system. According to the recorded statistics, 219 transactions were confirmed in approximately 17 minutes and 32 seconds,. On average, it took 0.24 minutes to confirm the transaction. The aggregate transaction fee was 00.767 Ether, while the average transaction fee was 0.01097 Ether. The list of accomplishments associated with the use of blockchain technology is extensive in terms of combating rampant fraud. This system greatly outperforms previous systems in terms of usability and efficiency. The blockchain technology method is an excellent solution since it works seamlessly with the existing credential verification ecosystem.

8.3 Limitations

One of the limitations of decentralised applications is maintenance because code and data posted on the blockchain are not easy to modify. DApps can be more difficult to manage than native apps, as the code and data broadcast to the blockchain are more difficult to edit. Once deployed, it's difficult for developers to update their DApps (or the underlying data kept by a DApp) - even if problems or security threats are discovered in an older version. This process, other than being difficult, is also expensive. Every time a smart contract is deployed on the blockchain, there will be an execution fee. Every programming error can be time-consuming and costly to rectify. Scalability of the blockchain and network congestion is another limitation of utilising blockchain in our solution. There is a significant performance cost and scaling is difficult. Each node executes and stores each transaction in order to accomplish the security, integrity, transparency, and reliability that Ethereum strives to. Additionally, proof-of-work takes time. When a single DApp consumes an excessive amount of computing resources, the entire network becomes backed up. At the moment, the network can process approximately 10-15 transactions per second; if more transactions are introduced faster than this, the pool of unconfirmed transactions would grow rapidly [29].

A further limitation is centralisation. Solutions created on top of Ethereum's base layer that is user- and developer-friendly may appear to be centralised services. For example, such services could store keys or other sensitive information on the server, use a centralised server to offer a frontend or conduct critical functions on a centralised server before writing to the blockchain. As a result, many of the benefits of blockchain over the previous paradigm are lost due to centralised control [83].

Transaction cost is one of the limitations we encountered in this research. Over the six months of the system test, the price of ether has risen continuously and rapidly, as evidenced by the results of our analysis in the previous section. Ether is the second-largest cryptocurrency by market capitalisation. However, this popularity has come at a cost for

transactions on this blockchain that are exceptionally high. This, in turn, may have a negative impact on the usability and effectiveness of the system.

The sample size was one of the limitations of this thesis. At different stages of this research, I had to collect data from participants to analyse it and study the results. Unfortunately, due to the COVID-19 pandemic, the response rate to the invitations reached the minimum limit in every study conducted in this thesis.

8.4 Future Research

This section introduces a number of future research possibilities that might be investigated in order to improve and extend the work described in this thesis. The following are the possibilities:

1. **Improving the Blockchain-Based Trusted Achievement Record System:** Chapters 4 and chapter 5 proposed the system as a general and extendable framework. Therefore, the current version of the Trusted Achievement Record System is designed based on model public blockchains and contains models for the most popular public blockchain (Ethereum). However, to tackle the limitations provided in section 8.3, it is an opportunity for future researchers to refine the Trusted Achievement Record System using private blockchains such as Hyperledger Fabric.

2. **Learning Model:** One of our proposed system's objectives is to help individuals plan their learning futures. We have succeeded in providing them with a trusted record of their achievements through the system we proposed. Therefore, the information about their achievements is essential to guide them to the best way to learn and tracks what would be the most appropriate for their interests. However, making decisions for a suitable learning plan is not automated in the current stage, which means users can build their plans by themselves based on the information in their achievement record. Thus, future researchers will have a great opportunity to study possible ways to automate this task.

3. **Updating the Systematic Mapping Study:** To follow up on the latest improvements and updates of adopting the blockchain and smart contracts innovation within the education field in general and in the higher education system in specific. We can add more questions to the study to identify more details relevant to design purposes, gaps, and future works. The study provides the research community with essential data and information that shortcut the way for researchers and facilitate investigating for appropriate solutions.

4. **Extending the system services:** This proposed system was developed to be extendable. Therefore, adopting new tasks or services will increase the system's feasibility. In addition, artificial intelligence (AI) methods could provide more potential use cases to the system, for example, finding the most appropriate student for the job based on the achievement record in the system, where the AI methods can link students' skills to the job requirements.

The proposed model is globalised and could be adopted to verify documents and build trusted records for users. For example, in health care, the model is suitable for creating a trusted patient record that can be verified and shared in a trusted and secure manner. Furthermore, the supply chain could adopt the model to generate trusted records for tracking and monitoring products. In general, the proposed model can be applied to create trusted records and for verifying purposes in many fields.Technically, the work presented in this thesis would provide help and shortcut the effort of any researcher developing solutions based on blockchain and smart contracts technologies. In terms of components, tools, mechanisms and use case scenarios, this thesis provides guidelines on how those parts are chosen and integrated. Therefore, the method designed for this research is generalised and suitable for any similar research. Furthermore, future researchers can adopt the findings of any conducted study or work in this thesis to develop new decentralised solutions.

References

[1] Abdinnour-Helm, S. F., Chaparro, B. S., and Farmer, S. M. (2005). Using the end-user computing satisfaction (eucs) instrument to measure satisfaction with a web site. *Decision Sciences*, 36(2):341–364.

[2] Al Harthy, K., Al Shuhaimi, F., and Al Ismaily, K. K. J. (2019). The upcoming blockchain adoption in higher-education: requirements and process. In *2019 4th MEC International Conference on Big Data and Smart City (ICBDSC)*, pages 1–5. IEEE.

[3] Alderson, C., Alderson, J. C., and Beretta, A. (1992). *Evaluating second language education*. Cambridge University Press.

[4] Alharby, M. and van Moorsel, A. (2020). Blocksim: An extensible simulation tool for blockchain systems. *Frontiers in Blockchain*, 3:28.

[5] Androulaki, E., Barger, A., Bortnikov, V., Cachin, C., Christidis, K., De Caro, A., Enyeart, D., Ferris, C., Laventman, G., Manevich, Y., et al. (2018). Hyperledger fabric: a distributed operating system for permissioned blockchains. In *Proceedings of the thirteenth EuroSys conference*, pages 1–15.

[6] Antonopoulos, A. M. (2017). *Mastering Bitcoin: Programming the Open Blockchain*. O'Reilly Media, Inc., 2nd edition.

[7] Armknecht, F., Karame, G. O., Mandal, A., Youssef, F., and Zenner, E. (2015). Ripple: Overview and outlook. In *International Conference on Trust and Trustworthy Computing*, pages 163–180. Springer.

[8] Armstrong, D., Gosling, A., Weinman, J., and Marteau, T. (1997). The place of inter-rater reliability in qualitative research: An empirical study. *Sociology*, 31(3):597–606.

[9] Arndt, T. and Guercio, A. (2020). Blockchain-based transcripts for mobile higher-education. *International Journal of Information and Education Technology*, 10(2).

[10] Aumasson, J.-P., Meier, W., Phan, R. C.-W., and Henzen, L. (2014). Blake2. In *The Hash Function BLAKE*, pages 165–183. Springer.

[11] Awaji, B., Solaiman, E., and Albshri, A. (2020a). Blockchain-based applications in higher education: A systematic mapping study. In *ACM conference proceedings (ISBN: 978- 1-4503-7575-7)*. ACM.

[12] Awaji, B., Solaiman, E., and Marshall, L. (2020b). Investigating the requirements for building a blockchain-based achievement record system. In *Proceedings of the 5th International Conference on Information and Education Innovations*, ICIEI 2020, page 56–60, New York, NY, USA. Association for Computing Machinery.

[13] B Ekbote, V Hire, P. M. and Sisodia, J. (2017). Blockchain based remittances and mining using cuda. page 908–911. IEEE the 2017 International Conference On Smart Technologies For Smart Nation.

[14] Barreto, P., Rijmen, V., et al. (2000). The whirlpool hashing function. In *First open NESSIE Workshop, Leuven, Belgium*, volume 13, page 14. Citeseer.

[15] Behren, R. v. and Wall, J. (2016-05-31). Digital wallet. Library Catalog: Google Patents.

[16] Benet, J. (2014). Ipfs-content addressed, versioned, p2p file system. *arXiv preprint arXiv:1407.3561*.

[17] Bergmark, D., Phempoonpanich, P., and Zhao, S. (2001). Scraping the acm digital library. In *ACM SIGIR Forum*, volume 35, pages 1–7. ACM New York, NY, USA.

[18] Block, A. (2022). Block.co api documentation. In *API Documentation*, volume 1, page 1. Block.io.

[19] Böhme, R., Christin, N., Edelman, B., and Moore, T. (2015). Bitcoin: Economics, technology, and governance. *Journal of economic Perspectives*, 29(2):213–38.

[20] Boone, H. N. and Boone, D. A. (2012). Analyzing likert data. *Journal of extension*, 50(2):1–5.

[21] Bore, N., Karumba, S., Mutahi, J., Darnell, S. S., Wayua, C., and Weldemariam, K. (2017). Towards blockchain-enabled school information hub. In *Proceedings of the Ninth International Conference on Information and Communication Technologies and Development*, page Article 19. Association for Computing Machinery.

[22] Braun, V. and Clarke, V. (2012). Thematic analysis. In *APA handbook of research methods in psychology, Vol 2: Research designs: Quantitative, qualitative, neuropsychological, and biological.*, APA handbooks in psychology®., pages 57–71. American Psychological Association, Washington, DC, US.

[23] Brooke, J. (1996). Sus: a "quick and dirty'usability. *Usability evaluation in industry*, 189.

[24] Budhiraja, S. and Rani, R. (2019). TUDocChain-securing academic certificate digitally on blockchain. In *International Conference on Inventive Computation Technologies*, pages 150–160. Springer.

[25] Buterin, V. (2013). A next generation smart contract & decentralized application platform (2013) whitepaper. *Ethereum Foundation*.

[26] Cappelli, P. (2019-05-01). Your approach to hiring is all wrong. *Online at: https://hbr.org/2019/05/recruiting, Harvard Business Review*.

[27] Chambers, R. (2002). *Participatory Workshops: A Sourcebook of 21 Sets of Ideas and Activities*. Routledge, London.

[28] Chatterjee, R. and Chatterjee, R. (2017). An overview of the emerging technology: Blockchain. In *2017 3rd International Conference on Computational Intelligence and Networks (CINE)*, pages 126–127. IEEE.

[29] Chauhan, A., Malviya, O. P., Verma, M., and Mor, T. S. (2018). Blockchain and scalability. In *2018 IEEE International Conference on Software Quality, Reliability and Security Companion (QRS-C)*, pages 122–128. IEEE.

[30] Chen, G., Xu, B., Lu, M., and Chen, N.-S. (2018). Exploring blockchain technology and its potential applications for education. *Smart Learning Environments*, 5(1):1.

[31] Chohan, U. W. (2017). The double spending problem and cryptocurrencies. *Available at SSRN 3090174*.

[32] Courage, C. and Baxter, K. (2005). *Understanding your users: A practical guide to user requirements methods, tools, and techniques*. Gulf Professional Publishing.

[33] Curmi, A. and Inguanez, F. (2018). BlockChain based certificate verification platform. In *International Conference on Business Information Systems*, pages 211–216. Springer.

[34] Czichos, H., Saito, T., and Smith, L. (2006). *Springer handbook of materials measurement methods*, volume 978. Springer.

[35] Dannen, C. (2017). *Introducing Ethereum and solidity*, volume 1. Springer.

[36] Dobbertin, H., Bosselaers, A., and Preneel, B. (1996). Ripemd-160: A strengthened version of ripemd. In *International Workshop on Fast Software Encryption*, pages 71–82. Springer.

[37] Doll, W. J. and Torkzadeh, G. (1988). The measurement of end-user computing satisfaction. *MIS quarterly*, pages 259–274.

[38] Doll WJ, T. G. (1988). The measurement of end-user computing satisfaction. *MIS quarterly*.

[39] Duffield, E. and Diaz, D. (2015). Dash: A privacycentric cryptocurrency. *online at https://docs.dash.org/en/stable/*.

[40] Durniak, A. (2000). Welcome to ieee xplore. *IEEE Power Engineering Review*, 20(11):12.

[41] E Androulaki, A Barger, V. B.-C. C. K. C. A. D. C. D. E. C. F. G. L. Y. M. S. M. C. M. B. N. M. S. G. S. K. S. A. S. C. S. M. V. S. W. C. and Yellick., J. (2017). Hyperledger fabric: A distributed operating system for permissioned blockchains. pages 1–15. ACMthe thirteenth EuroSys conference.

[42] Eaganathan, U., Indrian, V. V., and Nathan, Y. (2019a). Ideation framework of block chain adoption in malaysia higher education. In *Journal of Physics: Conference Series*, volume 1228, page 012072. IOP Publishing.

[43] Eaganathan, U., Indrian, V. V., and Nathan, Y. (2019b). Ideation framework of block chain adoption in malaysia higher education. In *Journal of Physics: Conference Series*, volume 1228, page 012072. IOP Publishing.

[44] Filvà, D. A., García-Peñalvo, F. J., Forment, M. A., Escudero, D. F., and Casañ, M. J. (2018). Privacy and identity management in learning analytics processes with blockchain. In *Proceedings of the Sixth International Conference on Technological Ecosystems for Enhancing Multiculturality*, pages 997–1003.

[45] Flick, U. (2018). *An introduction to qualitative research*. sage.

[46] Forment, M. A., Filvà, D. A., García-Peñalvo, F. J., Escudero, D. F., and Casañ, M. J. (2018). Learning analytics' privacy on the blockchain. In *Proceedings of the Sixth International Conference on Technological Ecosystems for Enhancing Multiculturality*, pages 294–298.

[47] Friend, M. and Cook, L. (1992). *Interactions: Collaboration skills for school professionals*. ERIC.

[48] Ghaffar, A. and Hussain, M. (2019a). BCEAP - a blockchain embedded academic paradigm to augment legacy education through application. In *Proceedings of the 3rd International Conference on Future Networks and Distributed Systems*, page Article 45. Association for Computing Machinery.

[49] Ghaffar, A. and Hussain, M. (2019b). BCEAP-a blockchain embedded academic paradigm to augment legacy education through application. In *Proceedings of the 3rd International Conference on Future Networks and Distributed Systems*, pages 1–11.

[50] Gibbs, T. and Yordchim, S. (2014). Thai perception on litecoin value. *International Journal of Social, Behavioral, Educational, Economic, Business and Industrial Engineering*, 8(8):2613–5.

[51] Gilbert, H. and Handschuh, H. (2003). Security analysis of sha-256 and sisters. In *International workshop on selected areas in cryptography*, pages 175–193. Springer.

[52] Gilbert, H. and Handschuh, H. (2004). Security analysis of sha-256 and sisters. In Matsui, M. and Zuccherato, R. J., editors, *Selected Areas in Cryptography*, pages 175–193, Berlin, Heidelberg. Springer Berlin Heidelberg.

[53] Gill, P., Stewart, K., Treasure, E., and Chadwick, B. (2008). Methods of data collection in qualitative research: interviews and focus groups. *British dental journal*, 204(6):291–295.

[54] Gillham, B. (2008). *Developing a questionnaire*. A&C Black.

[55] Global, A. (2022). Efmd global. In *Documentation*, volume 1, page 1. EFMD Global.

[56] Gresch, J., Rodrigues, B., Scheid, E., Kanhere, S. S., and Stiller, B. (2018). The proposal of a blockchain-based architecture for transparent certificate handling. In *International Conference on Business Information Systems*, pages 185–196. Springer.

[57] Han, M., Li, Z., He, J. S., Wu, D., Xie, Y., and Baba, A. (2018). A novel blockchain-based education records verification solution. In *Proceedings of the 19th Annual SIG Conference on Information Technology Education*, pages 178–183. Association for Computing Machinery.

[58] HEDD (2021). Higher education degree datacheck. *Online at https://hedd.ac.uk/*.

[59] Henle, C. A., Dineen, B. R., and Duffy, M. K. (2019). Assessing intentional resume deception: Development and nomological network of a resume fraud measure. *Journal of Business and Psychology*, 34(1):87–106.

[60] Herbert, W., Seliger, H. W., Shohamy, E. G., Shohamy, E., et al. (1989). *Second language research methods*. Oxford University Press.

[61] Hopwood, D., Bowe, S., Hornby, T., and Wilcox, N. (2016). Zcash protocol specification. *GitHub: San Francisco, CA, USA*, page 1.

[62] I Sukhodolskiy, S. Z. (2018). A blockchain-based access control system for cloud storage. In *IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering*, pages 1575–1578. IEEE.

[63] IMS (2022). Home | IMS Open Badges. *Online at https://openbadges.org/*.

[64] Initiative, M. M. L. L. (2016-10-25). Blockcerts-an open infrastructure for academic credentials on the blockchain. Library Catalog: medium.com.

[65] Ives, B., Olson, M. H., and Baroudi, J. J. (1983). The measurement of user information satisfaction. *Communications of the ACM*, 26(10):785–793.

[66] Jirgensons, M. and Kapenieks, J. (2018). Blockchain and the future of digital learning credential assessment and management. *Journal of Teacher Education for Sustainability*, 20(1):145–156.

[67] Juričić, V., Radošević, M., and Fuzul, E. (2019). Creating student's profile using blockchain technology. In *2019 42nd International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*, pages 521–525. IEEE.

[68] Kamišalić, A., Turkanović, M., Mrdović, S., and Heričko, M. (2019). A preliminary review of blockchain-based solutions in higher education. In *International Workshop on Learning Technology for Education in Cloud*, pages 114–124. Springer.

[69] Kanan, T., Obaidat, A. T., and Al-Lahham, M. (2019a). Smartcert blockchain imperative for educational certificates. In *2019 IEEE Jordan International Joint Conference on Electrical Engineering and Information Technology (JEEIT)*, pages 629–633.

[70] Kanan, T., Obaidat, A. T., and Al-Lahham, M. (2019b). SmartCert BlockChain imperative for educational certificates. In *2019 IEEE Jordan International Joint Conference on Electrical Engineering and Information Technology (JEEIT)*, pages 629–633. IEEE.

[71] Kaplowitz, M. D., Lupi, F., Couper, M. P., and Thorp, L. (2012). The effect of invitation design on web survey response rates. *Social Science Computer Review*, 30(3):339–349.

[72] Khandelwal, P., Johari, R., Gaur, V., and Vashisth, D. (2021). Blockchain technology based smart contract agreement on remix ide. In *2021 8th International Conference on Signal Processing and Integrated Networks (SPIN)*, pages 938–942. IEEE.

[73] Lam, T. Y. and Dongol, B. (2020). A blockchain-enabled e-learning platform. *Interactive Learning Environments*, pages 1–23.

[74] Lara, J. A., Aljawarneh, S., and Pamplona, S. (2020). Special issue on the current trends in e-learning assessment. *Journal of Computing in Higher Education*, 32(1):1–8.

[75] Lee, W.-M. (2019). Using the metamask chrome extension. In *Beginning Ethereum Smart Contracts Programming*, pages 93–126. Springer.

[76] Liu, L., Han, M., Zhou, Y., Parizi, R. M., and Korayem, M. (2020). Blockchain-based certification for education, employment, and skill with incentive mechanism. In *Blockchain Cybersecurity, Trust and Privacy*, pages 269–290. Springer.

[77] Liu, Q., Guan, Q., Yang, X., Zhu, H., Green, G., and Yin, S. (2018). Education-industry cooperative system based on blockchain. In *2018 1st IEEE International Conference on Hot Information-Centric Networking (HotICN)*, pages 207–211. IEEE.

[78] Liyuan, L., Meng, H., Yiyun, Z., and Reza, P. (2019). E^ 2 c-chain: A two-stage incentive education employment and skill certification blockchain. In *2019 IEEE International Conference on Blockchain (Blockchain)*, pages 140–147. IEEE.

[79] 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):109–134.

[80] M Mo ser, K Soska, E. H. K. L. H. H. S. S. K. H. J. H. A. M. A. N. N. C. (2019). An empirical analy- sis of traceability in the monero blockchain. pages 143—-163. Proceedings on Privacy Enhancing Technologies.

[81] Matzutt, R., Pennekamp, J., and Wehrle, K. (2020). A secure and practical decentralized ecosystem for shareable education material. In *2020 International Conference on Information Networking (ICOIN)*, pages 529–534. IEEE.

[82] Merriam, S. B. (1998). *Qualitative Research and Case Study Applications in Education. Revised and Expanded from" Case Study Research in Education.".* ERIC.

[83] Metcalfe, W. (2020). Ethereum, smart contracts, dapps. In *Blockchain and Crypt Currency*, pages 77–93. Springer, Singapore.

[84] Mitchell, I., Hara, S., and Sheriff, M. (2019). dAppER: Decentralised application for examination review. In *2019 IEEE 12th International Conference on Global Security, Safety and Sustainability (ICGS3)*, pages 1–14. IEEE.

[85] Molina-Jimenez, C., Sfyrakis, I., Solaiman, E., Ng, I., Wong, M. W., Chun, A., and Crowcroft, J. (2018a). Implementation of smart contracts using hybrid architectures with on and off–blockchain components. In *2018 IEEE 8th International Symposium on Cloud and Service Computing (SC2)*, pages 83–90. IEEE.

[86] Molina-Jimenez, C., Solaiman, E., Sfyrakis, I., Ng, I., and Crowcroft, J. (2018b). On and off-blockchain enforcement of smart contracts. In *European Conference on Parallel Processing*, pages 342–354. Springer.

[87] Mori, K. and Miwa, H. (2019). Digital university admission application system with study documents using smart contracts on blockchain. In *International Conference on Intelligent Networking and Collaborative Systems*, pages 172–180. Springer.

[88] Möser, M., Soska, K., Heilman, E., Lee, K., Heffan, H., Srivastava, S., Hogan, K., Hennessey, J., Miller, A., Narayanan, A., et al. (2018). An empirical analysis of traceability in the monero blockchain. *Proceedings on Privacy Enhancing Technologies*, 2018(3):143–163.

[89] NGA (2021). NGA human resources. Library Catalog: www.ngahr.com.

[90] Nguyen DH, Nguyen-Duc DN, H.-T. N. P. H. (2018). Cvss: A blockchainized certificate verifying support system. In *ACM conference proceedings (doi: 10.1145/3287921.3287968)*. ACM.

[91] Nunnaly, J. C. and Bernstein, I. H. (1978). Psychoneric theory. *Second Edion, McGraw-Hil*.

[92] Ocheja, P., Flanagan, B., Ueda, H., and Ogata, H. (2019). Managing lifelong learning records through blockchain. *Research and Practice in Technology Enhanced Learning*, 14(1):4.

[93] Patel, K. and Das, M. L. (2020). Transcript management using blockchain enabled smart contracts. In *International Conference on Distributed Computing and Internet Technology*, pages 392–407. Springer.

[94] Pennell, K. E. and Soraci, O. (1969). *Serrated edge coin separator with magnetic rail*. Google Patents.

[95] Petersen, K., Feldt, R., Mujtaba, S., and Mattsson, M. (2008). Systematic mapping studies in software engineering. In *12th International Conference on Evaluation and Assessment in Software Engineering (EASE) 12*, pages 1–10.

[96] Pishghadam, R., Zabihi, R., and Ghadiri, M. (2015). Linguistic-bound or life-wise language teaching beliefs: A mixed methods approach. *Current Psychology*, 34(4):654–665.

[97] Pope, C., Ziebland, S., and Mays, N. (2000). Analysing qualitative data. *Bmj*, 320(7227):114–116.

[98] Priya, N., Ponnavaikko, M., and Aantonny, R. (2020). An efficient system framework for managing identity in educational system based on blockchain technology. In *2020 International Conference on Emerging Trends in Information Technology and Engineering (ic-ETITE)*, pages 1–5. IEEE.

[99] Rahardja, U., Hidayanto, A. N., Hariguna, T., and Aini, Q. (2019). Design framework on tertiary education system in indonesia using blockchain technology. In *2019 7th International Conference on Cyber and IT Service Management (CITSM)*, volume 7, pages 1–4. IEEE.

[100] Richards, J. C. and Schmidt, R. W. (2013). *Longman dictionary of language teaching and applied linguistics*. Routledge.

[101] Rivest, R. and Dusse, S. (1992). The md5 message-digest algorithm. *MIT Laboratory for Computer Science Cambridge*.

[102] Sabharwal, N., Pandey, S., and Pandey, P. (2021a). Getting started with hashicorp automation solutions. In *Infrastructure-as-Code Automation Using Terraform, Packer, Vault, Nomad and Consul*, pages 1–10. Springer.

[103] Sabharwal, N., Pandey, S., and Pandey, P. (2021b). *Getting Started with Vault*, pages 131–150. Apress, Berkeley, CA.

[104] Sahonero-Alvarez, G. (2018). Blockchain and peace engineering and its relationship to engineering education. In *2018 World Engineering Education Forum-Global Engineering Deans Council (WEEF-GEDC)*, pages 1–6. IEEE.

[105] Sanmogan, E. (2018). How much does your CV lie? *Online at https://www.theukdomain.uk/much-cv-lie/*.

[106] Schmidt, P. (2016a). Blockcerts—an open infrastructure for academic credentials on the blockchain. *MLLearning (24/10/2016)*.

[107] Schmidt, P. (2016b). Blockcerts—an open infrastructure for academic credentials on the blockchain. *MLLearning (24/10/2016)*.

[108] Shariar, A., Imran, M. A., Paul, P., and Rahman, A. (2020). A decentralized computational system built on blockchain for educational institutions. In *Proceedings of the International Conference on Computing Advancements*, pages 1–6.

[109] Shen, H. and Xiao, Y. (2018). Research on online quiz scheme based on double-layer consortium blockchain. In *2018 9th International Conference on Information Technology in Medicine and Education (ITME)*, pages 956–960. IEEE.

[110] Solaiman, E., Wike, T., and Sfyrakis, I. (2020). Implementation and evaluation of smart contracts using a hybrid on- and off-blockchain architecture. *Concurrency and Computation: Practice and Experience*, n/a:e5811.

[111] Srivastava, A., Bhattacharya, P., Singh, A., Mathur, A., Prakash, O., and Pradhan, R. (2018). A distributed credit transfer educational framework based on blockchain. In *2018 Second International Conference on Advances in Computing, Control and Communication Technology (IAC3T)*, pages 54–59. IEEE.

[112] Szabo, N. (1994). Smart contracts. *Online at http:https://www.fon.hum.uva.nl/rob/Courses/ InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html*.

[113] T.-T Kuo, H Zavaleta Rojas, L. O.-M. (2019). Comparison of blockchain platforms: A systematic review and healthcare examples. *Journal of the American Medical Informatics Association*.

[114] Taha, A. and Zakaria, A. (2020). Truver: a blockchain for verifying credentials: poster. In *Proceedings of the 35th Annual ACM Symposium on Applied Computing*, pages 346–348.

[115] Todd, D. M. (2012). Workzone: Inquiries on rise amid resume fraud. *Pittsburgh Post Gazette*.

[116] Turkanović, M., Hölbl, M., Košič, K., Heričko, M., and Kamišalić, A. (2018). EduCTX: A blockchain-based higher education credit platform. *IEEE access*, 6:5112–5127.

[117] Vidal, F., Gouveia, F., and Soares, C. (2019). Analysis of blockchain technology for higher education. In *2019 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC)*, pages 28–33. IEEE.

[118] Viswanathan, R., Dasgupta, D., and Govindaswamy, S. R. (2019). Blockchain solution reference architecture (bsra). *IBM Journal of Research and Development*, 63(2/3):1–1.

[119] W Wang, D. T Hoang, P. H. Z. X. D. N. P. W. Y. W. D. I. K. (2019). A survey on consensus mechanisms and mining strategy management in blockchain networks. page 22328–22370. IEEE.

[120] Waclawski, E. (2012). How i use it: Survey monkey. *Occupational Medicine*, 62(6):477–477.

[121] Walport, M. (2016). Distributed ledger technology: Beyond blockchain. *UK Government Office for Science*, 1.

[122] Wang, L., Wang, X., Fu, J., and Zhen, L. (2008). A novel probability binary particle swarm optimization algorithm and its application. *J. Softw.*, 3(9):28–35.

[123] Watters, A. (2016). The blockchain for education: an introduction. *Online at http://hackeducation. com/2016/04/07/blockchain-education-guide*.

[124] Wessling, F., Ehmke, C., Meyer, O., and Gruhn, V. (2019). Towards blockchain tactics: Building hybrid decentralized software architectures. In *2019 IEEE International Conference on Software Architecture Companion (ICSA-C)*, pages 234–237. IEEE.

[125] Wöhrer, M., Zdun, U., and Rinderle-Ma, S. (2021). Architecture design of blockchain-based applications. In *2021 3rd Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS)*, pages 173–180. IEEE.

[126] Wood, G. (2014). Ethereum: A secure decentralised generalised transaction ledger. *Ethereum project yellow paper*, 151(2014):1–32.

[127] Wood, G. (2016). Polkadot: Vision for a heterogeneous multi-chain framework. *White Paper*, 21:2327–4662.

[128] Wood, G. (2019). Ethereum: A secure decentralised generalised transaction ledger. *online at https://ethereum.github.io/yellowpaper/paper.pdf*.

[129] Yumna, H., Khan, M. M., Ikram, M., and Ilyas, S. (2019). Use of blockchain in education: A systematic literature review. In *Asian Conference on Intelligent Information and Database Systems*, pages 191–202. Springer.

[130] Yusnita, Y., Eriyanti, F., Engkizar, E., Anwar, F., Putri, N. E., Arifin, Z., and Syafril, S. (2018). The effect of professional education and training for teachers (plpg) in improving pedagogic competence and teacher performance. *Tadris: Jurnal Keguruan dan Ilmu Tarbiyah*, 3(2):123–130.

[131] Zachman, J. A. (1987). A framework for information systems architecture. *IBM systems journal*, 26(3):276–292.

[132] Zhao, G., Di, B., and He, H. (2020a). Design and implementation of the digital education transaction subject two-factor identity authentication system based on blockchain. In *2020 22nd International Conference on Advanced Communication Technology (ICACT)*, pages 176–180. IEEE.

[133] Zhao, G., He, H., and Di, B. (2020b). Design and implementation of the digital education resources authentication system based on blockchain. In *Proceedings of the 2020 4th International Conference on Cryptography, Security and Privacy*, pages 100–104.

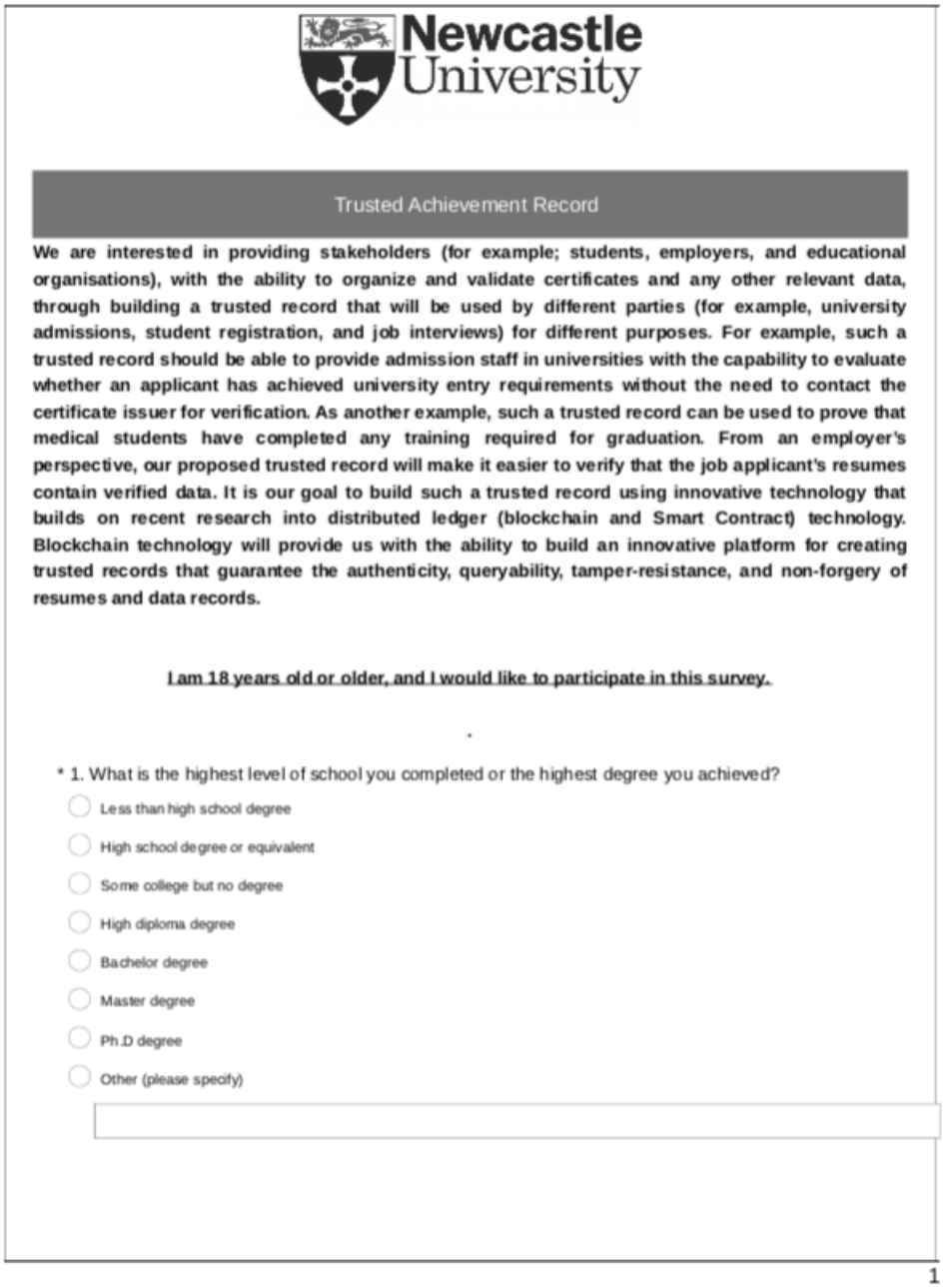
[134] Zhao, W., Yang, S., Luo, X., and Zhou, J. (2021). On peercoin proof of stake for blockchain consensus. In *2021 The 3rd International Conference on Blockchain Technology*, pages 129–134.

[135] Zimina, D. and Mouromtsev, D. (2020). Applying blockchain technology for improvement of the educational process in terms of data processing1.

[136] Zohrabi, M. (2013). Mixed method research: Instruments, validity, reliability and reporting findings. *Theory & practice in language studies*, 3(2).

Appendix A

Investigation the requirements Questionnaire



Newcastle University

Trusted Achievement Record

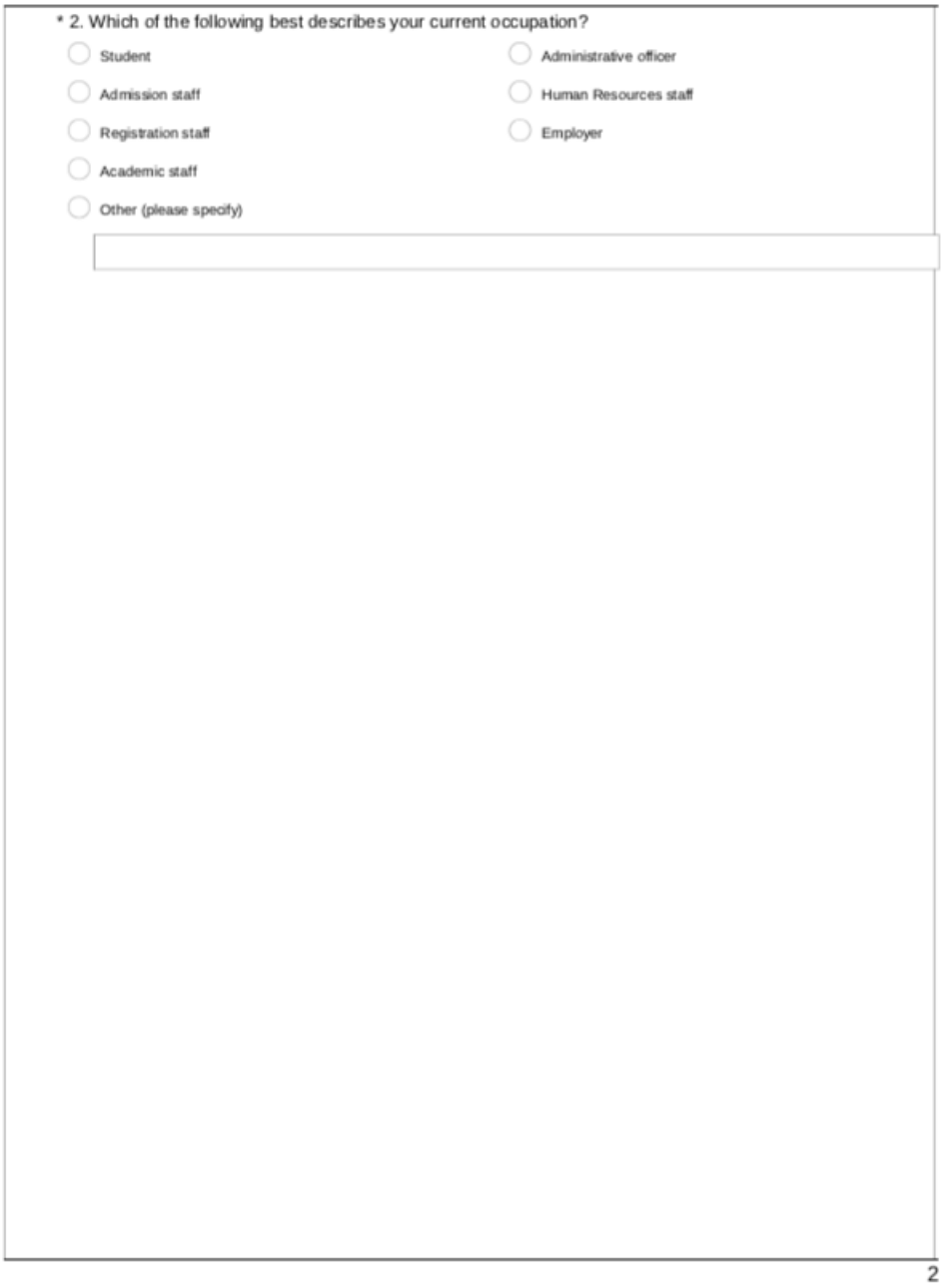
We are interested in providing stakeholders (for example; students, employers, and educational organisations), with the ability to organize and validate certificates and any other relevant data, through building a trusted record that will be used by different parties (for example, university admissions, student registration, and job interviews) for different purposes. For example, such a trusted record should be able to provide admission staff in universities with the capability to evaluate whether an applicant has achieved university entry requirements without the need to contact the certificate issuer for verification. As another example, such a trusted record can be used to prove that medical students have completed any training required for graduation. From an employer's perspective, our proposed trusted record will make it easier to verify that the job applicant's resumes contain verified data. It is our goal to build such a trusted record using innovative technology that builds on recent research into distributed ledger (blockchain and Smart Contract) technology. Blockchain technology will provide us with the ability to build an innovative platform for creating trusted records that guarantee the authenticity, queryability, tamper-resistance, and non-forgery of resumes and data records.

I am 18 years old or older, and I would like to participate in this survey.

* 1. What is the highest level of school you completed or the highest degree you achieved?

- Less than high school degree
- High school degree or equivalent
- Some college but no degree
- High diploma degree
- Bachelor degree
- Master degree
- Ph.D degree
- Other (please specify)

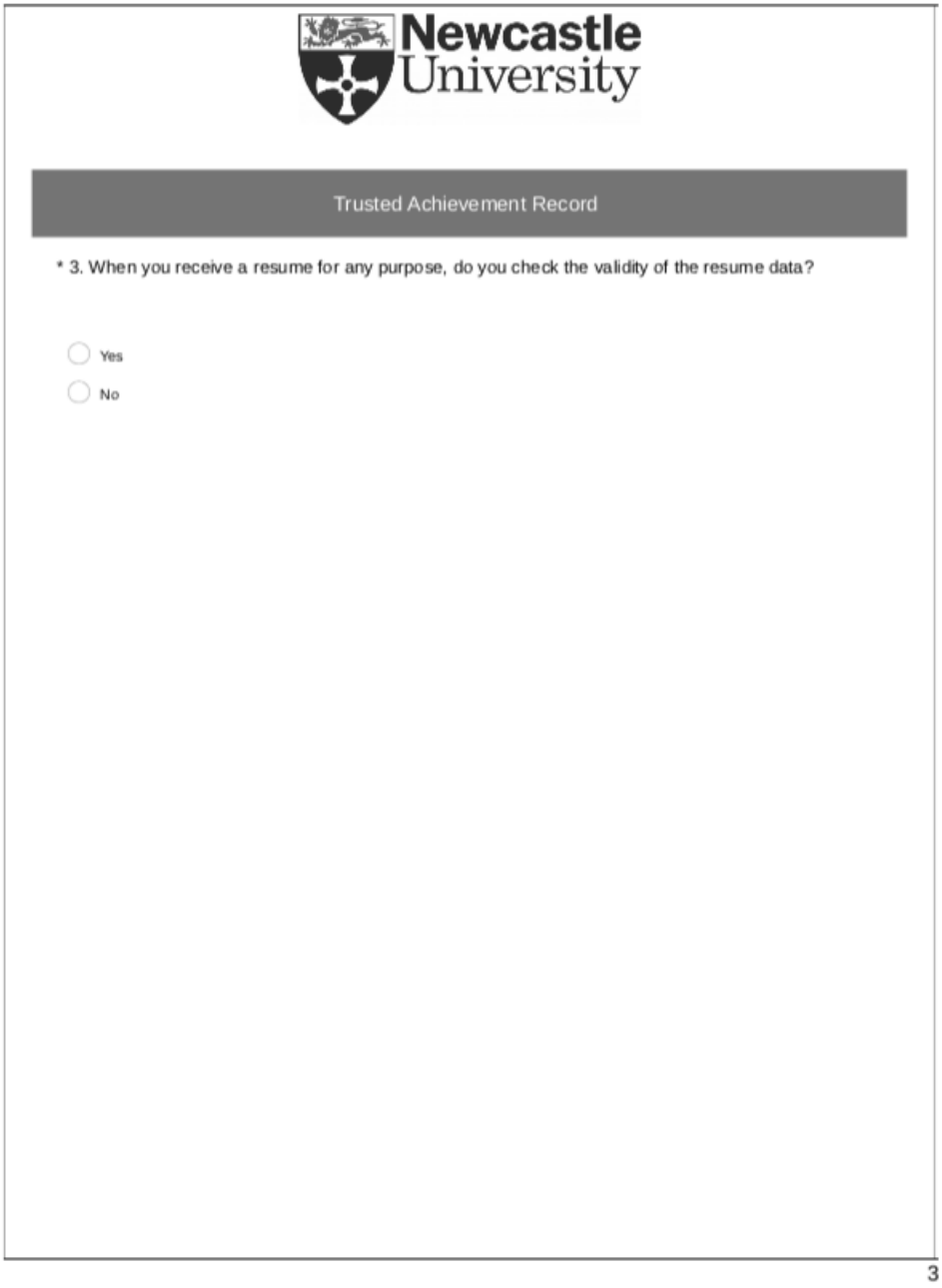
1

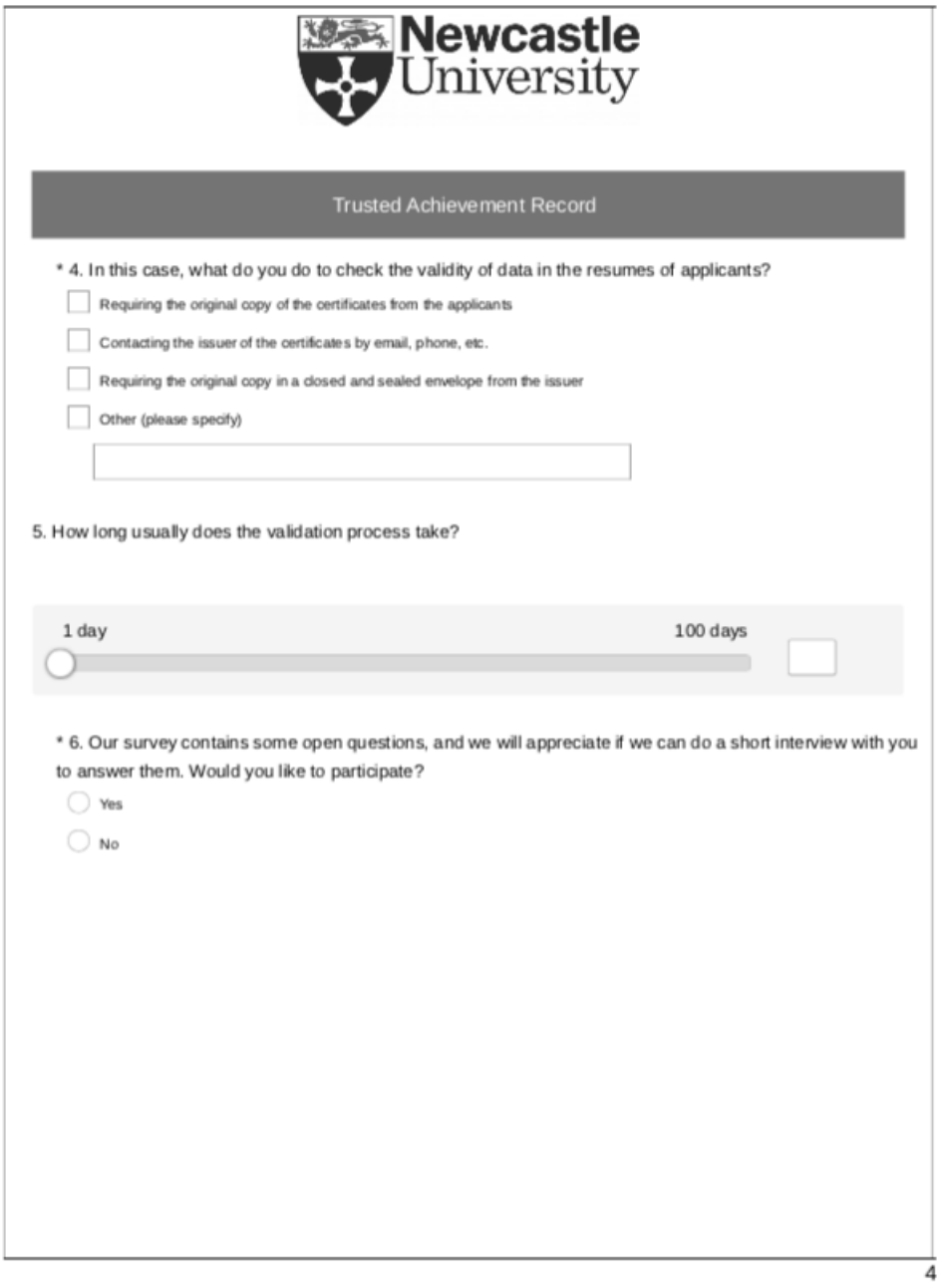


* 2. Which of the following best describes your current occupation?

- Student
- Admission staff
- Registration staff
- Academic staff
- Other (please specify)
- Administrative officer
- Human Resources staff
- Employer

2


Newcastle University
Trusted Achievement Record
* 3. When you receive a resume for any purpose, do you check the validity of the resume data?
Yes
No
3



Newcastle University

Trusted Achievement Record

* 4. In this case, what do you do to check the validity of data in the resumes of applicants?

- [ ] Requiring the original copy of the certificates from the applicants
- [ ] Contacting the issuer of the certificates by email, phone, etc.
- [ ] Requiring the original copy in a closed and sealed envelope from the issuer
- [ ] Other (please specify)

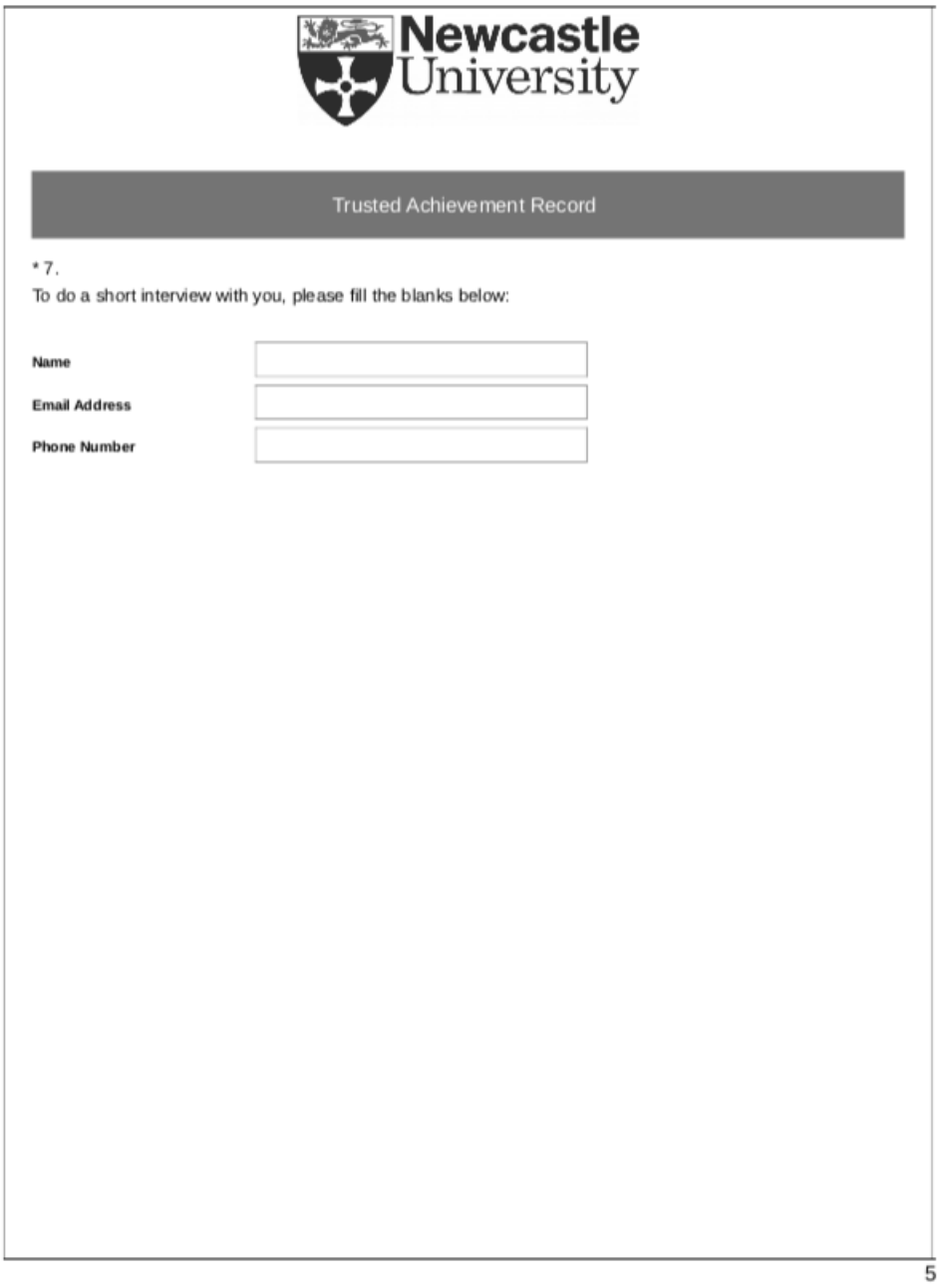
5. How long usually does the validation process take?

1 day — 100 days

* 6. Our survey contains some open questions, and we will appreciate if we can do a short interview with you to answer them. Would you like to participate?

- ( ) Yes
- ( ) No

4



Newcastle University

Trusted Achievement Record

* 7.

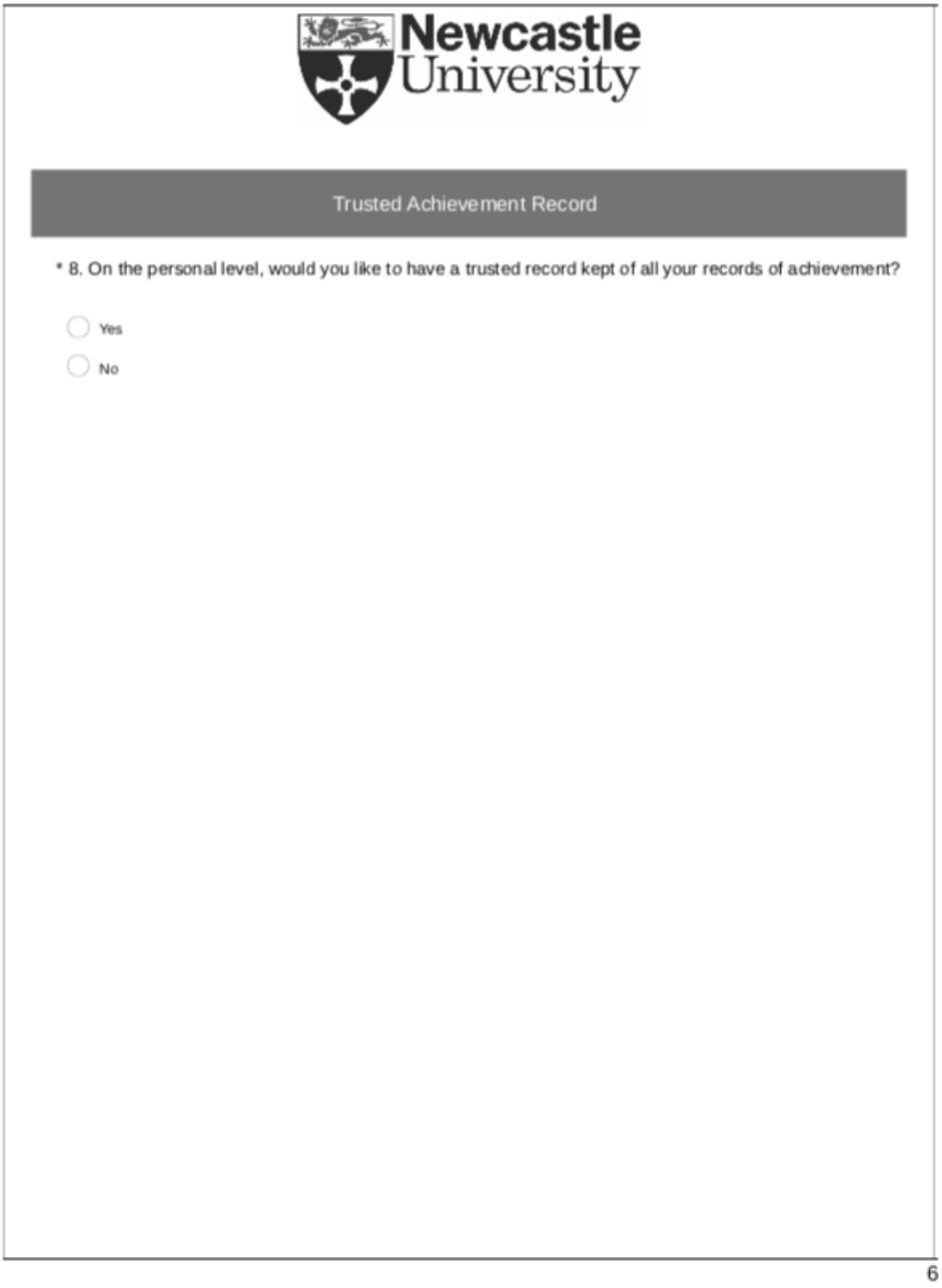
To do a short interview with you, please fill the blanks below:

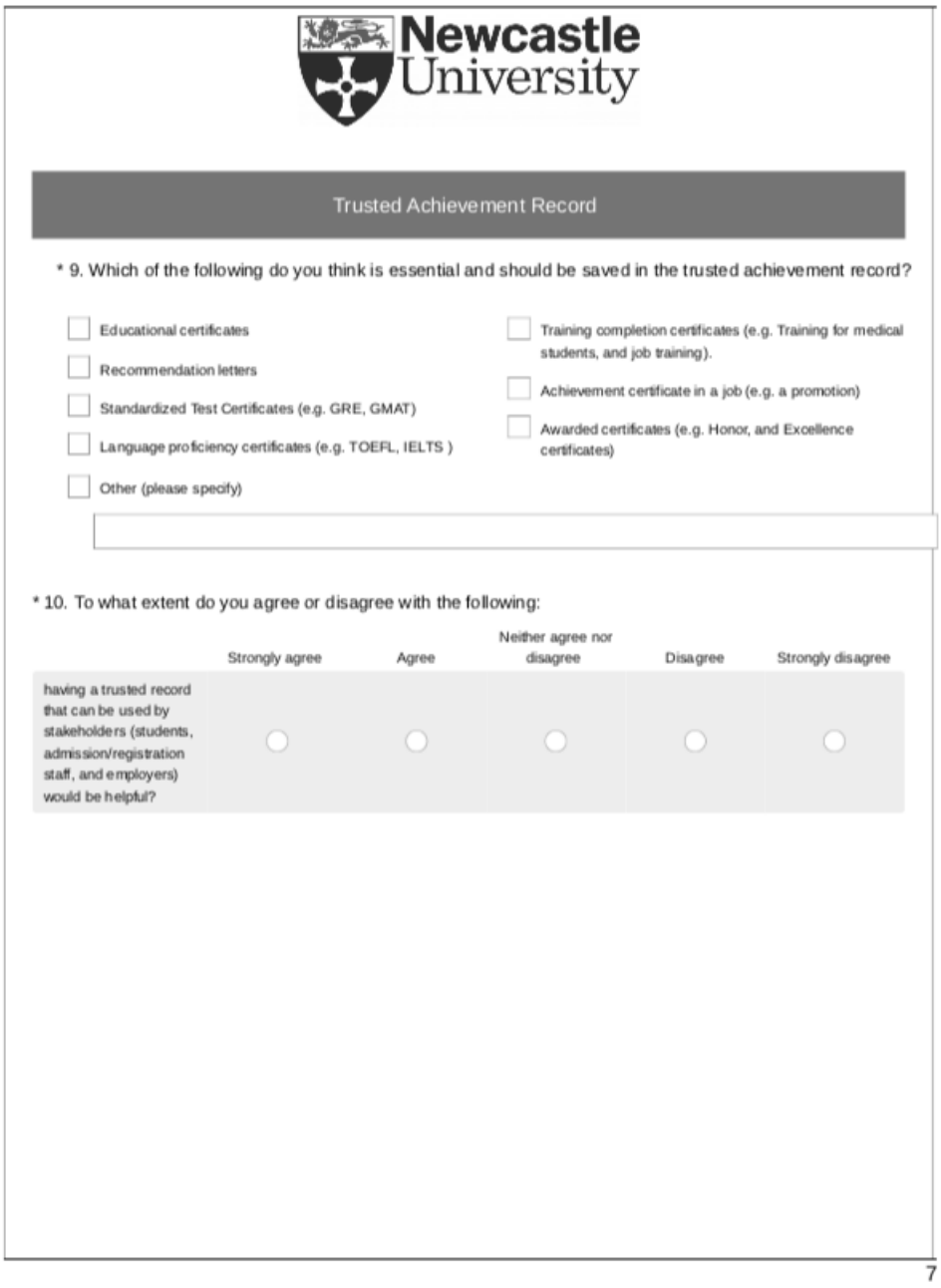
Name

Email Address

Phone Number

5


Newcastle University
Trusted Achievement Record
* 8. On the personal level, would you like to have a trusted record kept of all your records of achievement?
Yes
No
6



Newcastle University

Trusted Achievement Record

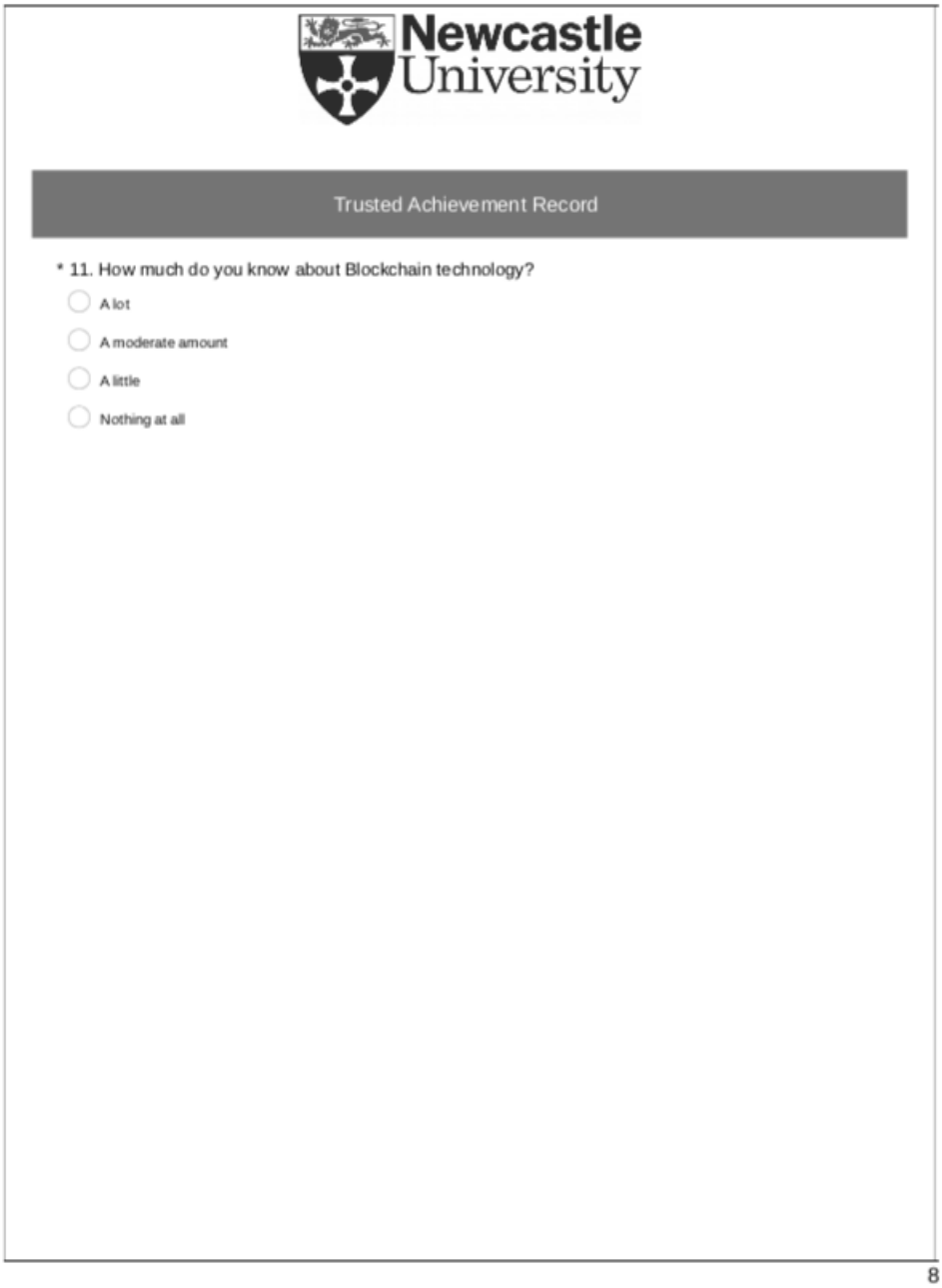
* 9. Which of the following do you think is essential and should be saved in the trusted achievement record?

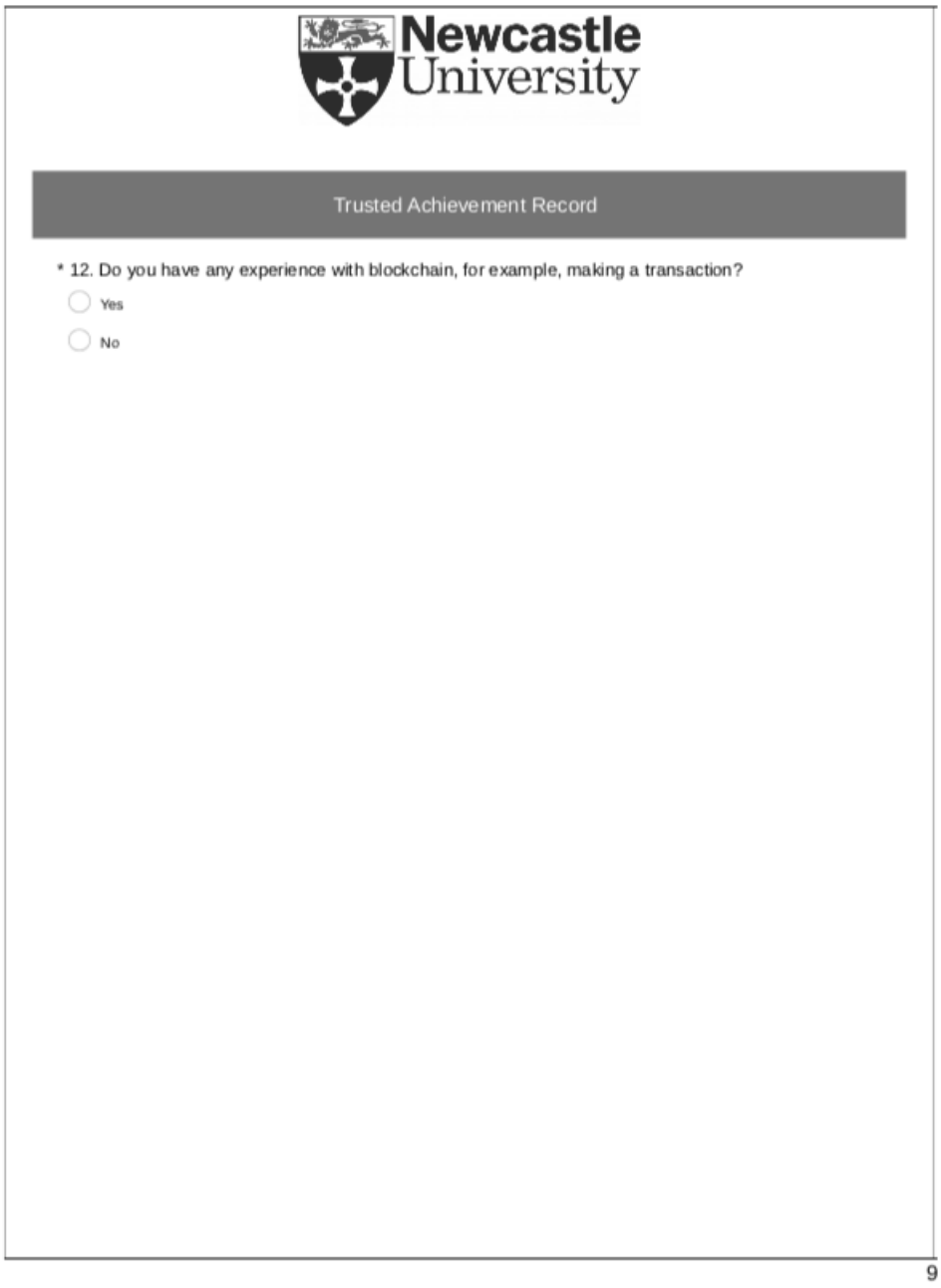
- [ ] Educational certificates
- [ ] Recommendation letters
- [ ] Standardized Test Certificates (e.g. GRE, GMAT)
- [ ] Language proficiency certificates (e.g. TOEFL, IELTS)
- [ ] Other (please specify)
- [ ] Training completion certificates (e.g. Training for medical students, and job training).
- [ ] Achievement certificate in a job (e.g. a promotion)
- [ ] Awarded certificates (e.g. Honor, and Excellence certificates)

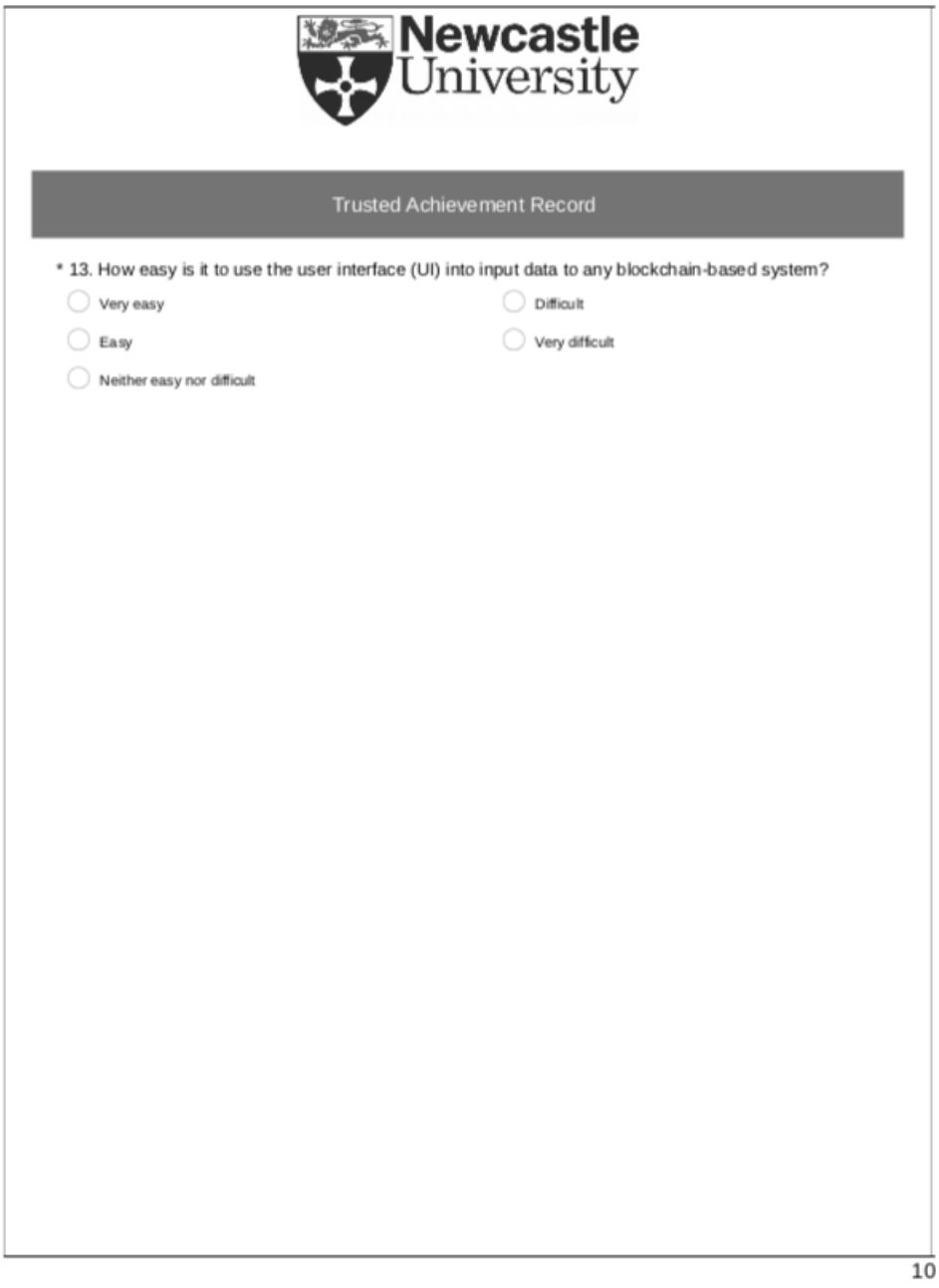
* 10. To what extent do you agree or disagree with the following:

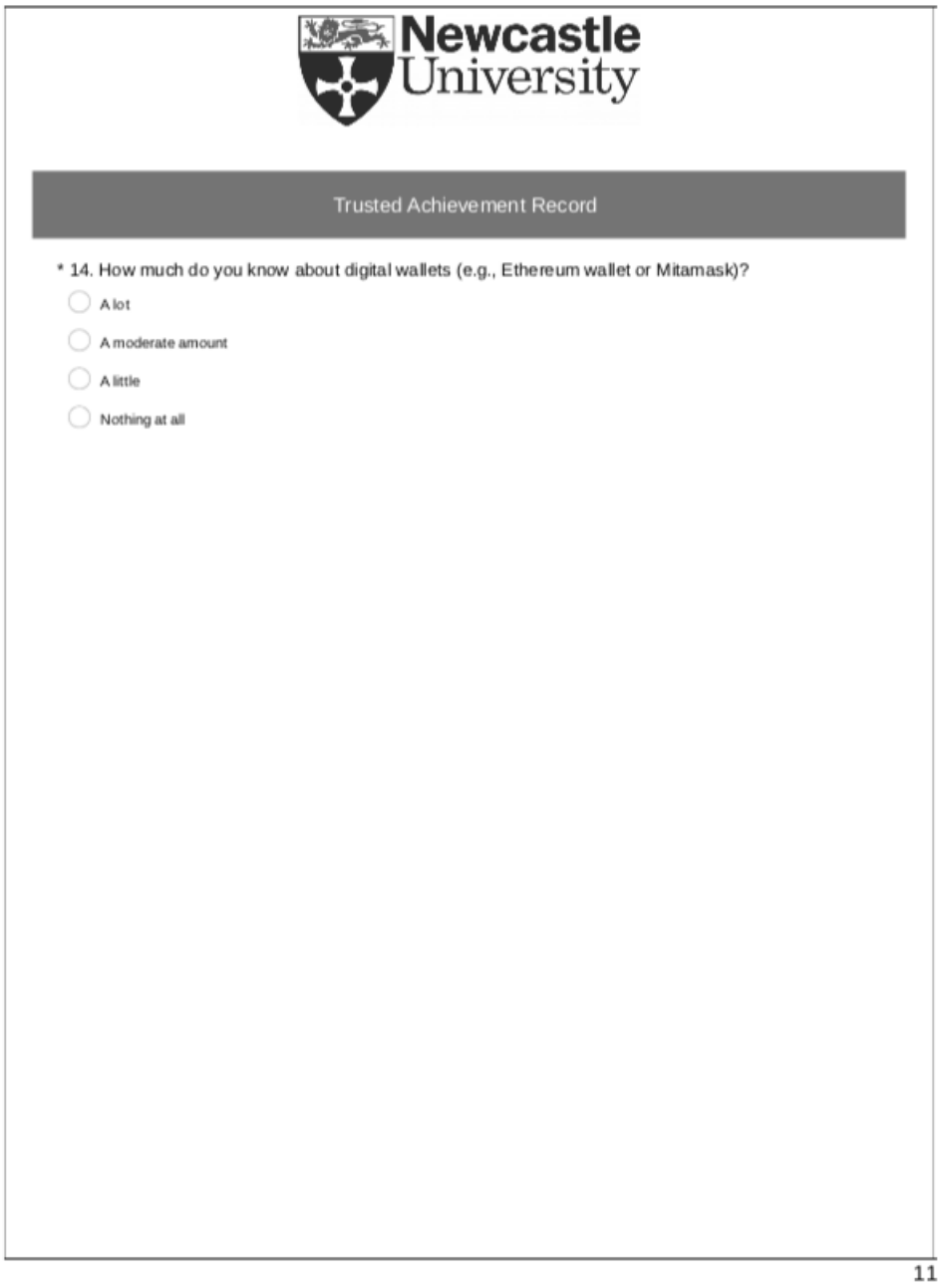
	Strongly agree	Agree	Neither agree nor disagree	Disagree	Strongly disagree
having a trusted record that can be used by stakeholders (students, admission/registration staff, and employers) would be helpful?	○	○	○	○	○

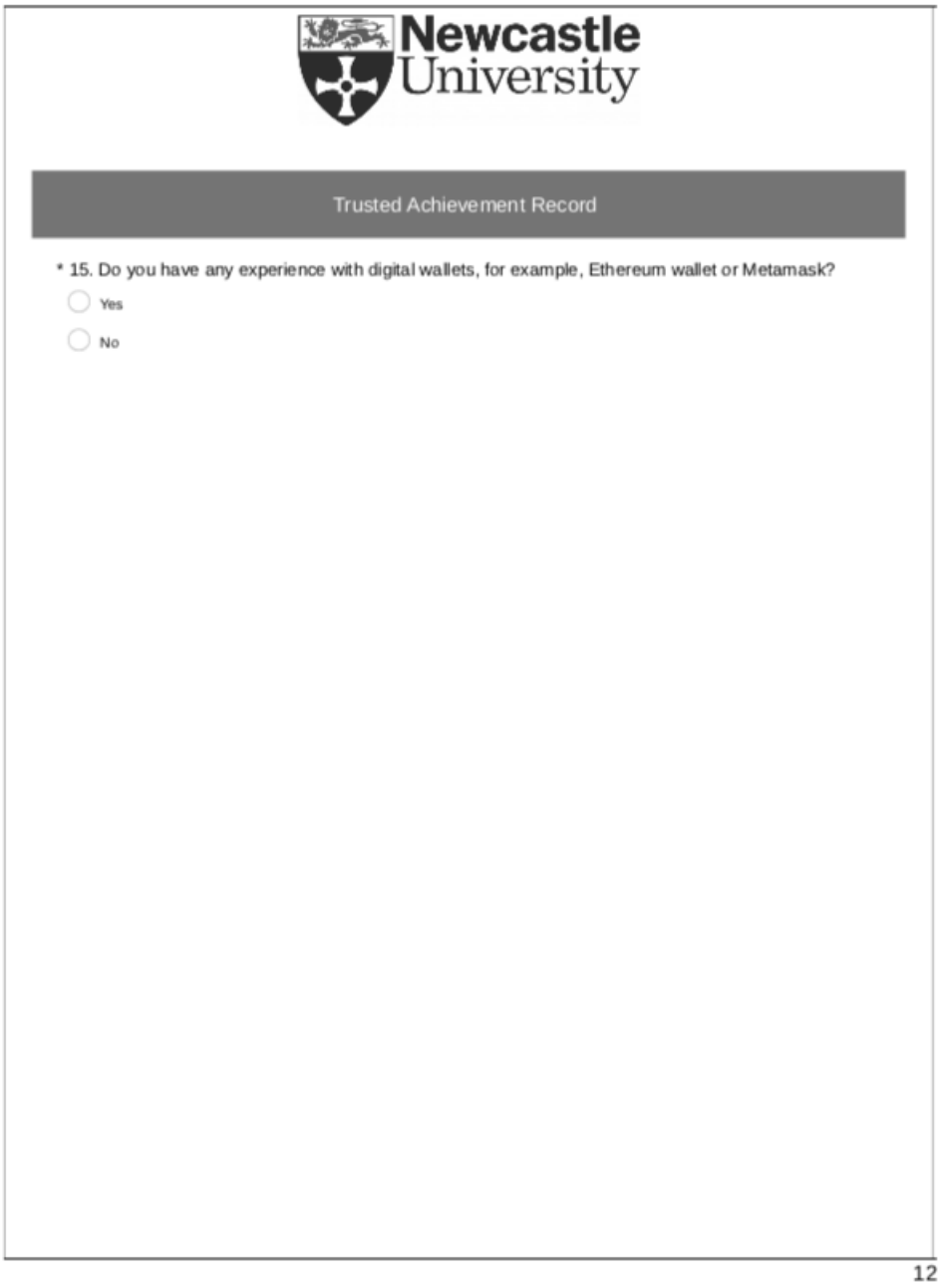
7

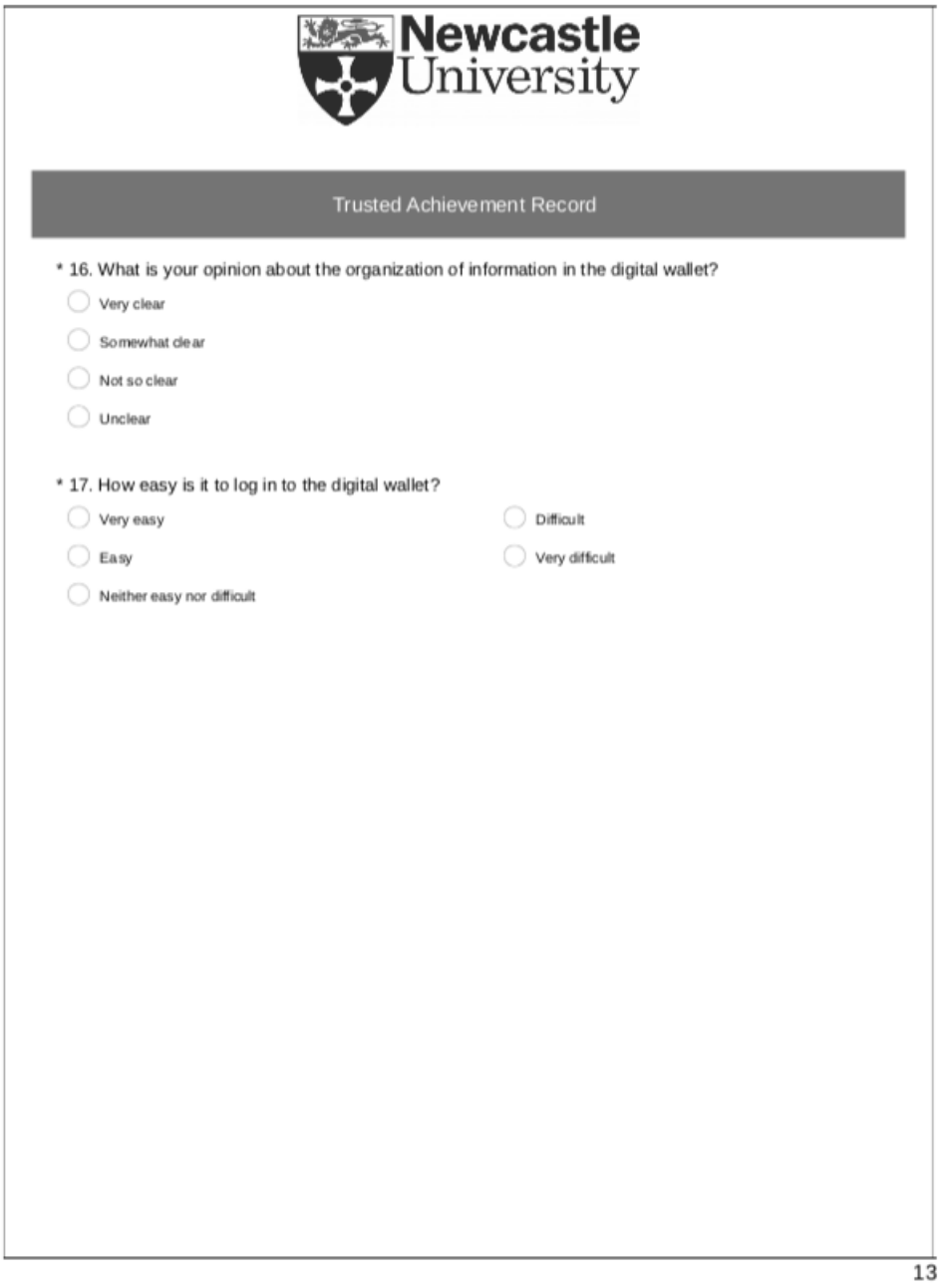

Newcastle University
Trusted Achievement Record
* 11. How much do you know about Blockchain technology?
A lot
A moderate amount
A little
Nothing at all
8


Newcastle University
Trusted Achievement Record
* 12. Do you have any experience with blockchain, for example, making a transaction?
Yes
No
9


Newcastle University
Trusted Achievement Record
* 13. How easy is it to use the user interface (UI) into input data to any blockchain-based system?
Very easy
Easy
Neither easy nor difficult
Difficult
Very difficult
10


Newcastle University
Trusted Achievement Record
* 14. How much do you know about digital wallets (e.g., Ethereum wallet or Mitamask)?
A lot
A moderate amount
A little
Nothing at all
11


Newcastle University
Trusted Achievement Record
* 15. Do you have any experience with digital wallets, for example, Ethereum wallet or Metamask?
Yes
No
12



Newcastle University

Trusted Achievement Record

* 16. What is your opinion about the organization of information in the digital wallet?

- Very clear
- Somewhat clear
- Not so clear
- Unclear

* 17. How easy is it to log in to the digital wallet?

- Very easy
- Easy
- Neither easy nor difficult
- Difficult
- Very difficult

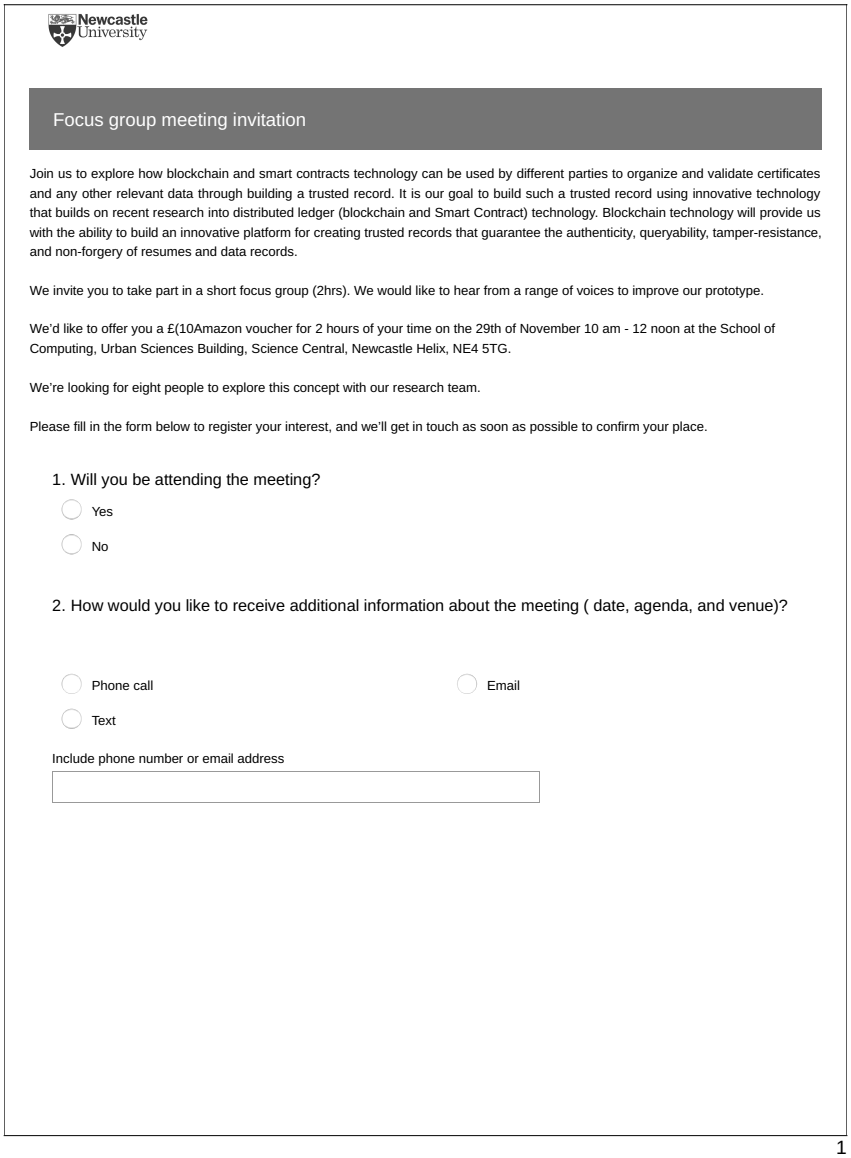
13


Newcastle University
Trusted Achievement Record
End of the survey
Thanks a lot for your participation.
14

Appendix B

Critique Workshop

1. The Invitation



Newcastle University

Focus group meeting invitation

Join us to explore how blockchain and smart contracts technology can be used by different parties to organize and validate certificates and any other relevant data through building a trusted record. It is our goal to build such a trusted record using innovative technology that builds on recent research into distributed ledger (blockchain and Smart Contract) technology. Blockchain technology will provide us with the ability to build an innovative platform for creating trusted records that guarantee the authenticity, queryability, tamper-resistance, and non-forgery of resumes and data records.

We invite you to take part in a short focus group (2hrs). We would like to hear from a range of voices to improve our prototype.

We'd like to offer you a £(10Amazon voucher for 2 hours of your time on the 29th of November 10 am - 12 noon at the School of Computing, Urban Sciences Building, Science Central, Newcastle Helix, NE4 5TG.

We're looking for eight people to explore this concept with our research team.

Please fill in the form below to register your interest, and we'll get in touch as soon as possible to confirm your place.

1. Will you be attending the meeting?

- Yes
- No

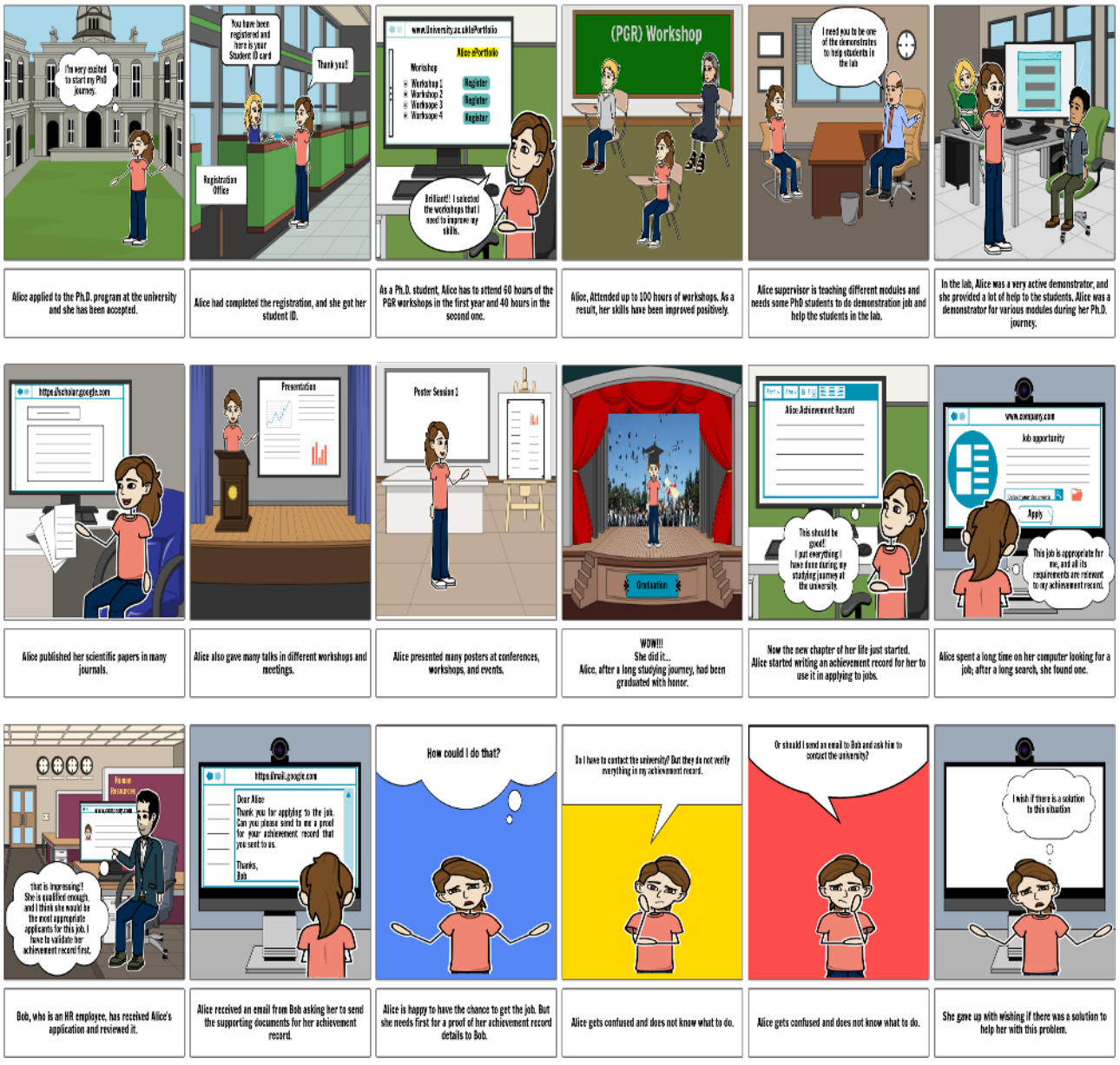
2. How would you like to receive additional information about the meeting (date, agenda, and venue)?

- Phone call
- Email
- Text

Include phone number or email address

1

2. The Storyboard



Alice applied to the Ph.D. program at the university and she has been accepted.

Alice had completed the registration, and she got her student ID.

As a Ph.D. student, Alice has to attend 60 hours of the PGR workshops in the first year and 40 hours in the second one.

Alice, Attended up to 100 hours of workshops. As a result, her skills have been improved positively.

Alice supervisor is teaching different modules and needs some PhD students to do demonstration job and help the students in the lab.

In the lab, Alice was a very active demonstrator, and she provided a lot of help to the students. Alice was a demonstrator for various modules during her Ph.D. journey.

Alice published her scientific papers in many journals.

Alice also gave many talks in different workshops and meetings.

Alice presented many posters at conferences, workshops, and events.

WOW!!!
She did it...
Alice, after a long studying journey, had been graduated with honor.

Now the new chapter of her life just started. Alice started writing an achievement record for her to use it in applying to jobs.

Alice spent a long time on her computer looking for a job; after a long search, she found one.

Bob, who is an HR employee, has received Alice's application and reviewed it.

Alice received an email from Bob asking her to send the supporting documents for her achievement record.

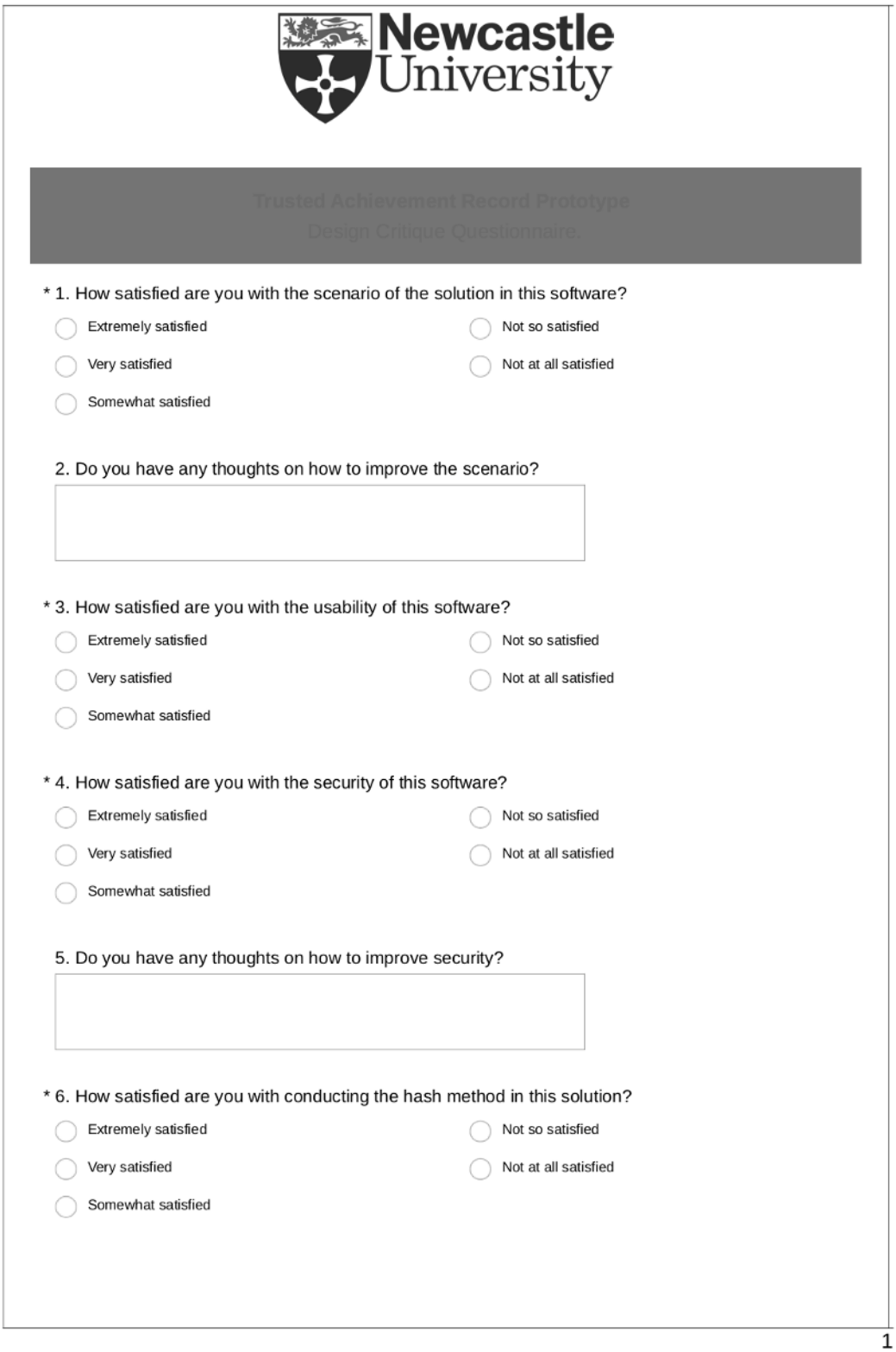
Alice is happy to have the chance to get the job. But she needs first for a proof of her achievement record details to Bob.

Alice gets confused and does not know what to do.

Alice gets confused and does not know what to do.

She gave up with wishing if there was a solution to help her with this problem.

3. The Critique Workshop Questionnaire



Newcastle University

Trusted Achievement Record Prototype

Design Critique Questionnaire.

* 1. How satisfied are you with the scenario of the solution in this software?

- Extremely satisfied
- Very satisfied
- Somewhat satisfied
- Not so satisfied
- Not at all satisfied

2. Do you have any thoughts on how to improve the scenario?

* 3. How satisfied are you with the usability of this software?

- Extremely satisfied
- Very satisfied
- Somewhat satisfied
- Not so satisfied
- Not at all satisfied

* 4. How satisfied are you with the security of this software?

- Extremely satisfied
- Very satisfied
- Somewhat satisfied
- Not so satisfied
- Not at all satisfied

5. Do you have any thoughts on how to improve security?

* 6. How satisfied are you with conducting the hash method in this solution?

- Extremely satisfied
- Very satisfied
- Somewhat satisfied
- Not so satisfied
- Not at all satisfied

1

* 6. How satisfied are you with conducting the hash method in this solution?

- Extremely satisfied
- Very satisfied
- Somewhat satisfied
- Not so satisfied
- Not at all satisfied

* 7. How satisfied are you with conducting the blockchain and smart contract in this solution?

- Extremely satisfied
- Very satisfied
- Somewhat satisfied
- Not so satisfied
- Not at all satisfied

* 8. How satisfied are you with including (public-blockchain) in this solution?

- Extremely satisfied
- Very satisfied
- Somewhat satisfied
- Not so satisfied
- Not at all satisfied

* 9. Do you think we should use (private- blockchain) instead of (public-blockchain)?

- Yes
- No

10. Do you have any thoughts on which blockchain type is best to conduct for this software?

* 11. How satisfied are you with the look and feel of this software?

- Extremely satisfied
- Very satisfied
- Somewhat satisfied
- Not so satisfied
- Not at all satisfied

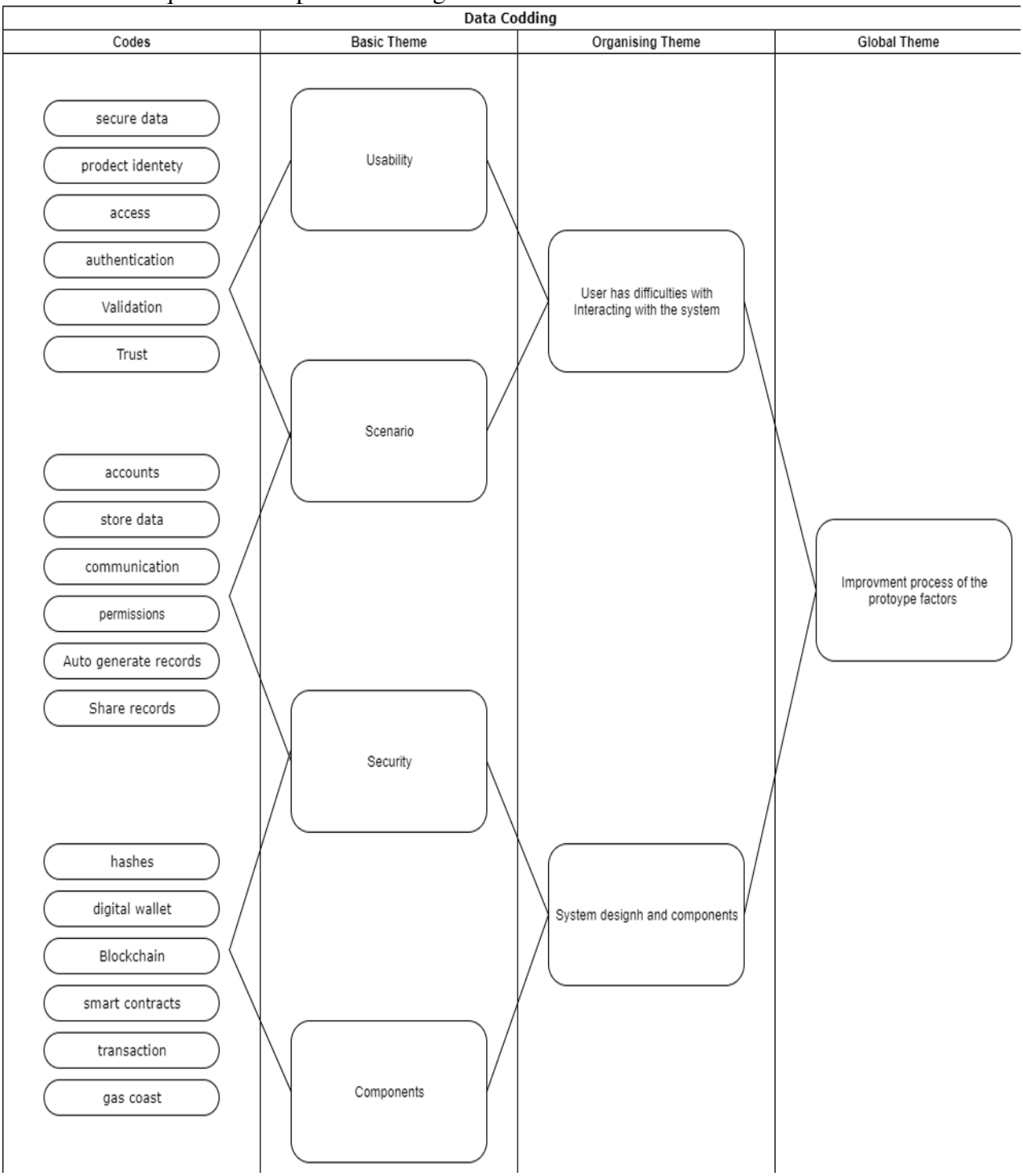
* 12. How satisfied are you with the communication way between users in this software?

- Extremely satisfied
- Very satisfied
- Somewhat satisfied
- Not so satisfied
- Not at all satisfied

13. Do you have any thoughts on how to improve the communication way between users in this software

14. Do you have any thoughts on how to improve this software?

4. The Critique Workshop Data Coding

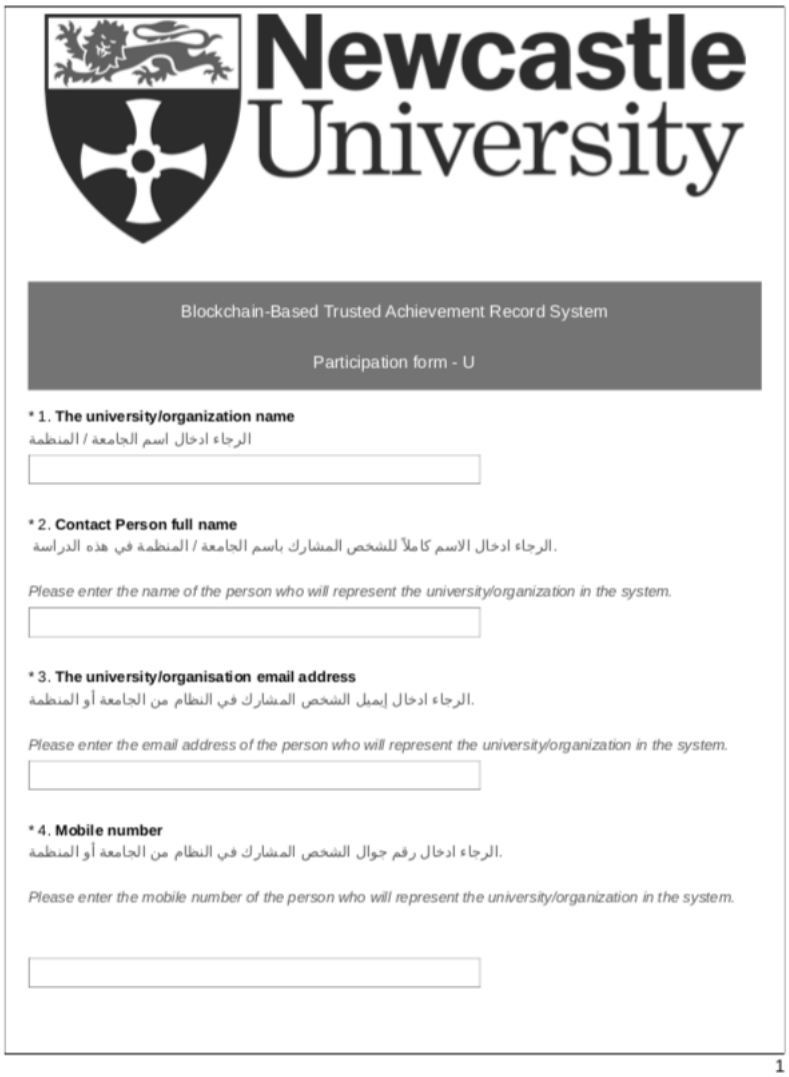


5. The meeting Place

Appendix C

Experimental Using the System by End-users

1. Universities Invitation Form



Newcastle University

Blockchain-Based Trusted Achievement Record System

Participation form - U

* 1. **The university/organization name**
الرجاء ادخال اسم الجامعة / المنظمة

* 2. **Contact Person full name**
الرجاء ادخال الاسم كاملاً للشخص المشارك باسم الجامعة / المنظمة في هذه الدراسة.

Please enter the name of the person who will represent the university/organization in the system.

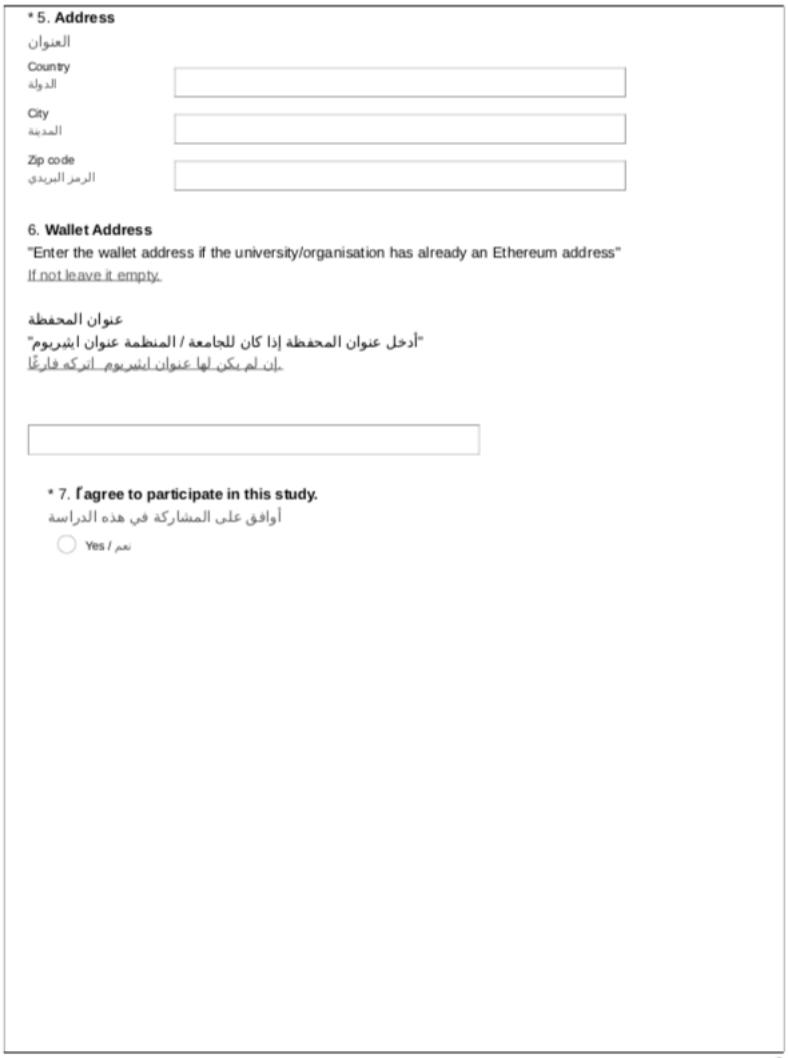
* 3. **The university/organisation email address**
الرجاء ادخال إيميل الشخص المشارك في النظام من الجامعة أو المنظمة.

Please enter the email address of the person who will represent the university/organization in the system.

* 4. **Mobile number**
الرجاء ادخال رقم جوال الشخص المشارك في النظام من الجامعة أو المنظمة.

Please enter the mobile number of the person who will represent the university/organization in the system.

1



* 5. **Address**

العنوان

Country
الدولة

City
المدينة

Zip code
الرمز البريدي

6. **Wallet Address**

"Enter the wallet address if the university/organisation has already an Ethereum address"
If not leave it empty.

عنوان المحفظة

"أدخل عنوان المحفظة إذا كان للجامعة / المنظمة عنوان ايثريوم"
إن لم يكن لها عنوان ايثريوم اتركه فارغًا.

* 7. **I agree to participate in this study.**

أوافق على المشاركة في هذه الدراسة

Yes / نعم

2

2. Invitation email

Invitation to Participate in System Evaluation

Bakri Awaji (PGR) <B.H.M.Awaji2@newcastle.ac.uk>
Tue 08/12/2020 23:43
To:

2 attachments (85 KB)
Ethical Approval statment.pdf; Bakri Evaluation Letter.pdf;

Dear :

I would like to invite you to participate in testing and evaluating the system that we have implemented and deployed.

This study is a part of a PhD research project conducted by Bakri Awaji, a doctoral candidate in the School of Computing at Newcastle University, to build a blockchain-based trusted achievement record system.

***How to participate:**

1. To participate in the evaluation process of the system, you need to fill the form in this link https://www.surveymonkey.co.uk/r/uform
2. Then, the system admin will register you to the system.
3. Once you are being registered in the system, the system will send an email to you contains the login information.
4. Next, you can access the system from this link http://18.130.174.71/index.php
5. Further information about the task you will practising within the system will be explained to you in a private Zoom meeting.
6. Students need to fill the form https://www.surveymonkey.co.uk/r/studentsform before participating.

*** Participants information:**
The Newcastle University Ethics Committee granted its approval for the project to progress.
By counting with this process, you give your consent for your results to be used as a part of this research. The participants' information will not be shared with anyone.
The data collected will be used by the researcher for testing and evaluating the system only.

***contacting information:**
If you would like further information about the research and the system then, please contact me via email: b.h.m.awaji2@newcastle.ac.uk

Kind Regards,

Bakri Awaji

Ph.D Candidate
School of Computing, TIG group
Newcastle University
Newcastle Upon Tyne
United Kingdom

Email b.h.m.awaji2@newcastle.ac.uk
personal mr.alawaji@gmail.com
Mobile +44 737 860 8666

3. Steps To participate Infographic