UNIVERSITY OF TECHNOLOGY SYDNEY

Faculty of Engineering and Information Technology

Intelligent Blockchain for Managing Micro-credentials (IBMM)

By

Hada Awaduilah Alsobhi

A THESIS SUBMITTED IN FULFILLMENT OF THE REQUIREMENTS FOR THE DEGREE

Doctor of Philosophy

Sydney, Australia

April 2024

CERTIFICATE OF ORIGINAL AUTHORSHIP

I, Hada Alsobhi declare that this thesis is submitted in fulfillment of the requirements for the award of Doctor of Philosophy, in the School of Computer Science/Faculty of Engineering and Information Technology at the University of Technology Sydney.

This thesis is wholly my own work unless otherwise referenced or acknowledged. In addition, I certify that all information sources and literature used are indicated in the thesis.

This document has not been submitted for qualifications at any other academic institution.

This research is supported by the Australian Government Research Training Program.

SIGNATURE: Production Note: Signature removed prior to publication.

DATE: April 2024

ACKNOWLEDGMENTS

I would like to start by offering my sincere gratitude to Allah, who guided me on this journey and who cast a light on the path leading to my goals, giving me the strength and resilience to reach my research destination, and providing me with this opportunity to complete my doctoral dissertation.

First and foremost, I would like to convey my heartfelt thanks and genuine appreciation to my thesis supervisor, Professor Farookh Hussain, for his unwavering guidance, patience, and expertise throughout this research endeavour. His mentorship has been invaluable, shaping not only the trajectory of this thesis but also my growth as a scholar.

Furthermore, I owe a debt of gratitude to my family for their continuous support, understanding, and assistance throughout this challenging journey. Their belief in me sustained my motivation and determination. My heartfelt appreciation goes to my parents, may Allah bless their souls, my husband, Dr Rayed Alakhtar, and my son, Abdulrahman. I can never thank you enough for your unwavering support and the sacrifices you made for me. Your kind words and unwavering belief in me were crucial in enabling me to complete this thesis. To my sisters and brothers, without their emotional support, this accomplishment would not have been possible. To my friends and colleagues who provided academic support, thank you for being a source of inspiration and camaraderie.

I would like to express my gratitude and thanks to Taif University for granting me the opportunity to finish my doctoral degree, the Saudi Arabian Cultural Mission (SACM) in Australia for supporting me during my Ph.D. journey, and the University of Technology Sydney (UTS) for granting me the opportunity to pursue my studies within its nurturing environment, which became a second home to me.

Lastly, I extend my appreciation to all the participants who generously shared their time and insights for this research. Your contributions were instrumental in shaping the findings of this study.

This thesis represents the culmination of years of dedication, hard work, and collaboration. It is a testament to the collective effort of those who believed in me and supported my academic pursuits. I am profoundly grateful for each and every one of you.

List of Publications

Journal Papers :

1. Alsobhi, Hada A., Rayed A. Alakhtar, Ayesha Ubaid, Omar K. Hussain, and Farookh Khadeer Hussain. "Blockchain-based micro-credentialing system in higher education institutions: Systematic literature review." Knowledge-Based Systems (2023): 110238. (JCR Q1 Journal).

2. Almadani, Mwaheb S., Suhair Alotaibi, Hada Alsobhi, Omar K. Hussain, and Farookh Khadeer Hussain. "Blockchain-based multi-factor authentication: A systematic literature review." Internet of Things (2023): 100844. (JCR Q1 Journal).

3. Alsobhi, Hada A. and Farookh Khadeer Hussain, "Intelligent Blockchain for Managing Micro-credentials (IBMM)", (Under preparation).

Conference Papers:

4. Alsobhi, Hada, et al. "Innovative Blockchain-Based Applications-State of the Art and Future Directions." International Conference on Advanced Information Networking and Applications. Cham: Springer International Publishing, 2021.

5. Alakhtar, Rayed, Sam Ferguson, and Hada Alsobhi. "User Expectations When Augmented Reality Mediates Historical Artifacts." International Conference on Advanced Information Networking and Applications. Cham: Springer International Publishing, 2022.

6. Alotaibi, Suhair, Hada Alsobhi, Ming Zhao, and Farookh Khadeer Hussain. "Blockchain for Identity: Ensuring Trust and Integrity in Education".IEEE International Conference on E-Business Engineering (ICEBE) 2023, (Accepted).

Abstract

Recently, blockchain technology or distributed ledger technology (DLT) has been used in a wide range of fields as a way to preserve records and information in a distributed and trusted manner. Blockchain technology has revolutionized higher education, particularly in the area of micro-credentials. The incorporation of micro-credentials in higher education has the potential to change traditional education and learning process. A number of micro-credentials can be accumulated for credit toward a specific academic degree. Validating micro-credentials is a time-consuming and cumbersome process, but blockchain technology enables students' micro-credentials to be validated easily and quickly. The immutability, decentralization, security, and transparency of blockchain technology make it a suitable technology for addressing the significant challenges associated with micro-credential provenance and data sharing in a secure manner. Several existing micro-credential platforms that use blockchain technology to efficiently and securely manage students' micro-credentials and academic accomplishments have been discussed in the literature. However, none of these existing platforms offer a comprehensive solution that can securely store, manage, and share micro-credentials with stakeholders in a privacy-preserving manner, nor are they able to provide personalized recommendations on students' majors and action plans.

In this thesis, we propose an intelligent blockchain for managing micro-credentials (IBMM) framework as a holistic platform for higher education students to manage their micro-credentials. A systematic literature review (SLR) was carried out to identify the shortcomings of the existing scientific studies in the micro-credential management area and to identify the research questions and solutions. By employing the SLR process, 15 relevant studies were identified and systematically reviewed which highlighted a number of research gaps. None of the existing studies propose a method that ensures the anonymity of students' identities on the blockchain when exchanging micro-credentials. Moreover, no intelligent techniques are used to recommend suitable majors for students and assist them in selecting the best action plan. This thesis examines the use of privacy-

preserving and AI methods to address these research gaps. Blockchain and AI techniques are integrated into the IBMM framework to undertake the following tasks:

- verify and store micro-credentials on the blockchain ledger to ensure the immutability and security of data.
- preserve the privacy of students' identities while sharing their micro-credentials with HEIs.
- recommend the most appropriate academic majors for students based on their micro-credentials.
- choose the most optimal action plan for students from multiple options based on several criteria.

In this thesis, research questions and objectives are identified, and an end-to-end solution is proposed to address the research issues.

Table of Contents

List of Figures

Figure **Page**

List of Tables

Table **Page**

CHAPTER 1

INTRODUCTION

1.1 Introduction

In this era of technological advancement and with its widespread use in educational institutions, students now have unprecedented access to learning opportunities. New online learning opportunities have also been introduced as a result of technological advancements, including short courses, digital certificates, degrees, learning recommendations, and micro-credentials [17]. The COVID-19 pandemic had a significant impact on the educational system, both locally and globally, and highlighted the need for lifelong learning [12]. Higher education institutions (HEIs) offer both formal and informal courses online, either fully or partially, to students from all over the world. The popularity of micro-credentials and online learning has changed the teaching and learning process in recent years. Students can earn micro-credentials online or in class to complete a specific degree. It is possible for the accumulated micro-credentials to be aggregated towards the achievement of a degree or diploma from a given institution [17].

Teaching and learning activities are mainly conducted through e-learning platforms at most HEIs. As a result of the widespread use of e-learning platforms during the pandemic, university students are better prepared to study online than they were previously [12]. Since most education tasks can be completed online, students do not have to attend class on campus or complete coursework to receive a degree. Therefore, many HEIs offer courses that focus on micro-credentials which have gained traction in many HEIs [17].

The integration of blockchain technology offers an ideal solution to develop a reliable micro-credential platform [58]. Blockchain technology, known for its scalability, reliability, and decentralized nature, holds significant potential for ensuring the credibility and security of micro-credentials [31]. Through the use of blockchain technology, HEIs can create a platform in which micro-credentials are verifiable, tamper-resistant, and globally acceptable, thus creating greater trust among students, employers, and HEIs [38].

To address the issues of micro-credential provenance, this thesis develops an intelligent and trustworthy higher education micro-credential platform based on blockchain technology for storing, managing, and verifying students' micro-credentials.

This chapter is structured as follows: Section 1.2 presents an overview of blockchain technology, micro-credentials, and blockchain-based micro-credentials. The subsections discuss blockchain technology in education and overview the components, features, types, and consensus models associated with blockchain. Section 1.3 overviews the thesis problem. Subsequently, Section 1.4 discusses the motivations behind this thesis, presenting the driving factors and rationale behind it. In Section 1.5, the thesis objectives are outlined, followed by a clear overview of what falls within the scope of the thesis in Section 1.6. Section 1.7 presents the important contributions of this thesis, with particular emphasis on its unique social and scientific significance to the field. Section 1.8 offers readers a snapshot of the content covered in each of the remaining seven chapters of this thesis. Section 1.9 concludes this chapter and provides a transition to the following chapter.

1.2 Background of the Thesis

1.2.1 Blockchain technology

Blockchain technology is a distributed database that stores transactions in sealed blocks and records them securely [89]. It stores cryptographically signed transactions in blocks on a ledger or chain. Upon a validation and consensus decision, each block is cryptographically linked to the prior one, which will lead to the continued growth of the chain [15]. Adding new blocks increases the resistance to tampering, making the modifiability of

older blocks difficult. Once a transaction is complete and written on the blockchain, data is impossible to change and tamper with [93]. Each block on the network is distributed among all copies of the ledger, and any conflicts are automatically resolved. There are three components to each block: the timestamp and hash of the preceding block, and the transaction [93]. Decentralized environments can be created using blockchain technology, which prevents third parties from controlling data and transactions [93]. Blockchain technology generally relies on a peer-to-peer (P2P) network to communicate and validate new blocks using a particular protocol [15]. P2P networks link a group of nodes together to form a blockchain. Several copies of the mutual ledger are maintained at each network node. Every node is capable of validating transactions, sending and receiving messages, and creating blocks [15].

1.2.2 Blockchain types

Blockchains can be classified into the following three types [15]:

1. Permissionless (Public Blockchain): permissionless blockchain networks are non-restrictive decentralized ledger systems that enable everyone on the network to publish blocks without requesting permission from a centralized authority. They are usually open-source software freely accessible and available to the public. As everyone has the authority to publish blocks on the blockchain, anyone can gain access to read, write to the ledger, and create blocks by joining the network as a node [93].

2. Permissioned (Private Blockchain): permissioned blockchain networks are restricted centralized systems that allow only authorized users to join the network [93]. They can restrict read access and who can create blocks. Due to the small size and limited scope of private networks, they are not accessible to the general public. All users must obtain permission before accessing them. There are typically only a few users who can participate in a private blockchain network, which is reserved for organizations and businesses. The governing organization determines authorizations and accessibility [15].

3. Consortium (Federated Blockchain): consortium blockchain networks are a combination of public and private blockchain networks; they are semi-decentralized and semi-private systems that allow only some nodes to join in the distributed consensus process [15]. There might be restrictions on reading and writing, certain

nodes will verify transactions. Consortium blockchains make transactions more private, scalable, and faster [73].

1.2.3 Blockchain components

This section explains the main components of blockchain to generate a secure digital environment. Breaking down and describing each component of blockchain technology simplifies the technology's complexity [93]. There are many blockchain components hence the following compilation of components may not be exhaustive; however, it is necessary to understand these components to grasp the concepts outlined in this thesis.

- Cryptographic Hash Functions: the process of hashing uses a cryptographic hash function to generate a digest or message digest from inputs of various sizes, such as files, text, or images [93]. The Secure Hash Algorithm (SHA256) is a cryptographic hash function that commonly appears in blockchain implementations with its output size of 256 bits. Blockchain technology uses a variety of cryptographic hash functions, not just SHA256. However, a wide range of computer hardware supports SHA-256, allowing fast and efficient computations [93].

- Transactions: the term "transaction" refers to an exchange or interaction among parties, such as transferring cryptocurrencies between users on the blockchain network [93]. Blockchain network security depends on creating new blocks continuously, even with no transactions. Transactions in smart contract systems can be used for sending, processing, and storing data on the blockchain. There can be differences in the data that make up a transaction between blockchain implementations. However, the transaction mechanism in which information is sent to the blockchain network by a blockchain network user remains the same [93]. The information sent potentially includes but is not limited to inputs and outputs of transactions, a sender's address and public key, and a digital signature. It is important to determine the validity and authenticity of a transaction no matter how data is generated and transmitted to ensure that the sender has access to the digital assets being sent [93].

- Ledger: a ledger includes a set of transactions, and nodes within the blockchain network are responsible for maintaining a ledger that records all transactions. A blockchain ledger shows the current status of data stored on the network [93].

- Wallets: blockchain wallets are digital wallets that serve as a secure repository to manage and store a user's private information, asymmetric keys, and transaction addresses. Blockchain users can purchase digital currencies or assets, sell them, and monitor their balances [73].

- Blocks: the transactions are appended to the blockchain ledger when a publisher issues a block [93]. A block comprises a block header and block data; the block header consists of information about this block, such as a block number, a hash value of the prior block header, a hash value of the block data, and a timestamp. The block data comprises a validated and genuine list of transactions submitted to the network [93].

- Smart Contracts: smart contracts, often known as digital contracts, are collections of code and data executed on blockchain networks using cryptographically signed transactions, such as Ethereum's smart contracts or Hyperledger Fabric's chaincode [93]. Blockchain nodes execute smart contracts; all nodes must obtain the same outcomes from the execution, and the outcomes of execution are stored on the blockchain. Users in a blockchain network are able to generate transactions that transmit data to a smart contract's public functions, and with the user-provided data, the smart contract executes the appropriate method to carry out a specific service [93]. Blockchain network users can encode their logic in the form of functions, and every time this function is invoked, it becomes a transaction on the blockchain [73]. Permissionless blockchain networks (such as Ethereum) that support smart contracts will charge a transaction fee for the cost of executing the smart contract code. On the other hand, permissioned blockchain networks (such as Hyperledger Fabric) that support chaincode do not require users to pay for the execution of smart contracts [93].

1.2.4 Blockchain consensus models

Consensus models are used in blockchain technology to allow a group of distrustful nodes to work together and decide or select which one is responsible for publishing the subsequent block [89]. While there are several approaches to selecting a node that can publish the next block, some of these approaches may be ineffective in terms of network longevity or even pose dangers to the network. Therefore, the basic idea of consensus models is to establish agreement on a specific node to avoid potential attacks on the network [89]. Upon nodes joining the blockchain network, they establish consensus on the

system's initial state, which is the only preconfigured block recorded in the genesis block [93]. Every blockchain network contains a genesis block, and each subsequent block must conform to the agreed-upon consensus model. It takes time to achieve agreement among all nodes, regardless of which distributed consensus protocol is used. It is necessary for every block to meet validation criteria, so every node within a blockchain network can verify it independently [93]. Blockchain technology provides several distributed consensus models and everyone has a different approach to selecting the node that can publish a new block. In the following, we provide three commonly used consensus models in blockchain technology to reach a consensus:

1. Proof of work (PoW) model: the PoW utilizes computational power in the Bitcoin network as a method to select the node that can publish the subsequent block [89]. Solving a computationally intensive puzzle successfully qualifies the node as the winner of the competition, with their solution serving as proof of their efforts. Nodes receive rewards when they win and bitcoins are added to their accounts. The puzzle is purposely designed to be difficult to solve, but validating a solution is simple [93]. All other full nodes can then easily validate a new block proposed to append it to the replicas, and blocks that do not satisfy the puzzle are rejected. As one of the most common puzzle techniques, a node competes by finding a hash digest of a block header that is smaller than a target value. This creates competition between nodes to discover a hash digest that matches the target [93]. In Bitcoin, the mining process is a PoW procedure and miners are the network nodes that compute the hash values [96].

2. Proof of stake (PoS) model: the PoS relies on the stake a node owns within the network. Nodes that have a higher stake in the system are more likely to want it to succeed and less likely to destroy it [93]. A stake is usually a cryptocurrency size that the blockchain network node has invested in the system. Blockchain networks based on PoS use stake size to determine a node's ability to publish new blocks. Consequently, the likelihood that a blockchain network node will publish a new block depends on the size of cryptocurrency staked in the network overall [93]. In contrast with PoW, PoS does not require energy consumption since the node competition is not based on computational power. PoS has several versions and DPoS is one of them that has a different mechanism on how to select a node responsible for publishing the next block [89].

3. Practical Byzantine Fault Tolerance (PBFT): the PBFT is a consensus algorithm used by Hyperledger Fabric to handle Byzantine faults. There is a possibility that up to one-third of malicious Byzantine replicas can be handled by PBFT [96]. Each round of the algorithm selects a node to publish the next block. There are three phases in the process, pre-prepared, prepared, and commit. A node may move on to the next phase if it receives votes from over two-thirds of the nodes. It is essential that the network knows every node in PBFT [96].

1.2.5 Blockchain features

Blockchain technology has several applications in different fields, such as education, banking, healthcare, etc. due to its various characteristics. The following are some common features of blockchain technology:

1. Blockchain technology is secure as it uses advanced cryptographic techniques, ensuring that data within the ledger can be authenticated and cannot be tampered with [93].

2. Blockchain technology has the principal characteristics of immutability and transparency, which ensures the integrity of educational credentials, stability, and unalterability. It also prevents fraud and unauthorized modifications as all the changes are visible to authorized users [15].

3. Blockchain technology operates on a distributed network that allows the number of nodes to be increased so they are more resilient to malicious attacks [93].

4. Blockchain technology operates on a decentralized network in which there is no centralized authority or individual governing it. This feature of blockchain and its consensus mechanisms protect it from hacking and unauthorized access [15].

5. Blockchain technology is a shared network in which the ledger is shared among numerous nodes, providing transparency [93].

6. Blockchain technology provides ownership and control of data in which students have full control over their educational records since they can decide what data to share, with whom, and when [15].

7. Blockchain technology can be an effective and reliable technique for enabling individuals and institutions to verify academic achievements and educational credentials securely without the need for intermediaries [15].

8. Blockchain technology uses smart contracts, which can manage several operations, such as enrolling students, distributing payment, completing courses, reducing administrative costs, and enhancing efficiency [15].

1.2.6 Blockchain in education

The education sector can be revolutionized by blockchain technology in several ways, including credential verification and data security. In addition to offering the technological means to decentralize online education, micro-credentials enable students to maintain their academic accomplishments throughout their lives. The technology also enables students, institutions, and employers to operate more efficiently, securely, and with more confidence. Certificates created and saved in the blockchain automatically become immutable, and once data is written on the ledger, it cannot be altered [70].

The most popular uses of blockchain technology are issuing, sharing, and verifying students' education qualifications (e.g., degrees, transcripts) and technical skills [15]. With blockchain technologies, the credential process is simplified and employers can verify an employee's academic performance quickly and easily. The use of blockchain in the education sector increases confidence and reduces costs by providing a secure platform for sharing student data [15]. In addition, a complete course record is stored using blockchain technology as chronologically ordered data blocks. Generating a blockchain-based infrastructure to keep track of academic credentials and accomplishments throughout a student's life is much more effective and secure than paper records [15].

The following examples illustrate the successful implementation of blockchain in the education sector:

- Blockcerts: the Massachusetts Institute of Technology (MIT) collaborated with Learning Machine to create Blockcerts, an open standard designed to develop, issue, and validate secure and tamper-proof blockchain-based educational credentials [9]. The Blockcerts Wallet app helps students quickly and easily obtain a secure and verified digital copy of their diploma. Moreover, this initiative empowers students to share their digital credentials with employers and institutions, significantly improving the efficiency and credibility of the verification process [26].
- Sony Global Education (SGE): this is an established educational blockchain-based platform resulting from a partnership with IBM, in which student records are

secured and shared using blockchain technology [45]. The collaboration between Sony Corporation and Sony Global Education aims to apply blockchain specifically to the education system. The collaboration focuses on streamlining administrative processes such as grade recording, attendance tracking, and course management, ensuring data integrity and reducing the risk of fraud through the decentralized nature of blockchain [64].

- QualiChain project: this project explores decentralized solutions for storing, sharing, and verifying education and employment qualifications, with a focus on leveraging blockchain technology, algorithmic techniques, and computational intelligence to disrupt public education, its connections to private education, the labor market, and administrative processes in the public sector [70]. Lifelong learning is a central target and the project aims to assist lifelong learners at various stages of their learning and career paths. The pilot case study specifically investigates how blockchain technologies can benefit lifelong learners by providing transparent and immutable educational accreditation, personalized recommendations based on their achievements, and support in attaining both personal and professional learning goals [71].

1.2.7 Micro-credentials

A micro-credential is a mini-qualification that provides evidence that skills, knowledge, and/or experience in a specific field or ability have been attained and it can be used by the student to progress towards a larger credential or degree that focuses on a particular field of study in the shortest amount of time [17, 31]. Micro-credentials are narrower in range and easier to acquire than traditional qualifications and are a useful alternative to a traditional degree. In the era of technology-based learning, micro-credentials have become increasingly popular. In education, micro-credentials will have a positive impact on learning engagement [17, 58]. Micro-credentials are a new area in the education sector that has expanded significantly over recent years and have become popular in the higher education sector [17, 31]. While several institutions offer online certification programs, only a few offer micro-credentials.

Before 2020, micro-credentials were available in a variety of forms, but their popularity grew as a result of the COVID-19 pandemic, which accelerated their implementation in many sectors [17, 61]. Since the COVID-19 pandemic, micro-credentials are the most

recent innovation in online education, gaining traction in public and private universities throughout the world. Micro-credentials, also known as digital badges, have recently emerged as a way to verify the completion of shorter, more specific learning courses that are not shown on academic transcripts [17, 55].

In June 2020, the Australian Government announced the creation of a Micro-credentials Marketplace for students to identify educational opportunities. The Australian Qualification Framework (AQF) 2019 sets common standards for micro-credentials across Australia and provides consistency and recognition of micro-credentials [4]. A number of international universities, including the University of Malaya, Notre Dame, Pennsylvania State University in the US, and the Open University in Europe, have created their own credit recognition or micro-credentialing policies. In Australia, a few universities, such as the University of Technology Sydney (UTS), Deakin, Griffith, and Swinburne University, have started offering micro-credentials in their respective institutions [12].

Several micro-credentials can be combined and students can choose where to acquire them, which allows them to achieve a large base of micro-credentials and eventually obtain a degree or diploma. Micro-credentials are beneficial to both students and higher education providers because they allow for the grouping of small learning attributes, such as soft skills, competencies, and professional skills [17]. As a result, students will be able to develop their skills and experience and are provided with a pathway to higher education to participate in continuous learning. Short courses with specific skills can help them upgrade their skills outside of the classroom. Upon completion of a short course, students are awarded a certificate as proof of completion [17, 51]. Despite this, there are issues associated with certificates, including how easy it is to alter them fraudulently. It is often a cumbersome and lengthy process to replace a certificate if it is lost, etc. [30, 58]. Furthermore, students who attend multiple short courses may also encounter difficulties in managing and presenting numerous certificates for other institutions [17, 31].

Micro-credentials offer many benefits for students. For instance, micro-credentials save the students' time by breaking a broad subject down into bite-sized pieces that they can easily consume while allowing students to acquire new skills in a time-efficient manner [17, 47]. Moreover, micro-credentials promote and support the pursuit of lifelong learning by allowing students to develop their skills and knowledge throughout their

lives. Learning with micro-credentials increases students' opportunities and provides them with the flexibility to learn at their own pace [17, 47]. Furthermore, the use of micro-credentials can also enhance learning experiences by offering students credentials for specific skills and additional skills and competencies obtained beyond education institutions [17, 47].

The lack of a common understanding of micro-credentials is a major hurdle to expanding the utilization of micro-credentials in higher education [17, 47]. Micro-credential platforms are crucial to the implementation of micro-credential initiatives in HIEs. Recently, micro-credential platforms have proliferated rapidly, and each one has its own features to meet the needs of its users [17, 47]. Since the topic is relatively new, the literature still does not cover all these platforms. The general idea behind micro-credential platforms is for users to be able to store, manage, share, and create online micro-credentials [17, 47]. However, in some cases, online credentials are manually verified or stored by a third party, causing administrative workload and making them vulnerable to forgery. As a potential solution, researchers have started integrating micro-credentials with blockchain technology in the last few years to overcome these issues [17, 58]. Therefore, to facilitate community acceptance of earning online micro-credentials, the creation of a trustworthy, secure, resilient, and scalable platform using blockchain technology is essential [12, 17].

1.2.8 Blockchain-based micro-credentials

Blockchain is an ideal technology to implement in relation to micro-credentials as it provides an infrastructure for managing, storing, and documenting the details of micro-credentials [17, 38]. Micro-credentials are a useful tool for students to show both what they can do today and their future potential, as blockchain technology can capture and communicate the skills and knowledge a student has previously attained. Micro-credentials are permanently secured and stored on a blockchain which guarantees that they cannot be changed. A blockchain is a decentralized approach where each student is given a reliable, unique, and persistent credentialing e-portfolio, which also gives the students full administrative control and authority over the credentials they have attained [17, 76]. Furthermore, blockchain permanently authenticates and stores micro-credentials while offering users full control and management over their credentials. It is impossible to hack blockchain in the traditional sense because it is a distributed ledger that has a high degree of security, so there is no possibility of micro-credentials being

forged [17, 76].

Since blockchain research is advancing quickly, a better understanding of blockchain's applications in the area of micro-credentialing will contribute to the future improvement of micro-credential platforms. However, there is still a lack of comprehensive software frameworks for HEIs, leaving usable, and reusable micro-credentialing applications in their early stages of development [17, 58].

Blockchain technology has characteristics that are advantageous for micro-credentials, as shown in Figure 1.1. This technology helps to solve many associated problems in the process of managing micro-credentials, which makes it a good fit to use with micro-credential platforms [17, 31].

Blockchain technology can improve the privacy of micro-credentials by providing anonymity. It uses a pseudonym (public key) that is unrelated to a user's real identity, so even if the transaction is disclosed on the blockchain, the user's identity cannot be determined [17, 35]. As previously mentioned, blockchain is a secure technology with an advanced level of encryption, so it can prevent micro-credentials from being forged [17, 88]. Since micro-credentials are stored on blocks in the blockchain ledger, and each block is cryptographically linked to the previous block, it is impossible to change or erase data once it is written on the blockchain, which also improves security and stability [17, 49]. As micro-credentials are stored permanently on the blockchain, students can utilize them indefinitely, which enhances their longevity and durability [17, 82]. Additionally, this technology can ensure credibility, integrity, and reliability for micro-credentials because all parties on the blockchain can trust that all transactions presented to the ledger are trustworthy by checking the credential timestamping [17, 49]. Thus, students can reliably share their micro-credentials, and other parties can validate the integrity of these micro-credentials on the blockchain because every party can participate in the transaction, so this also improves trust and transparency [17, 82]. Blockchain also can help to increase information availability for micro-credential recognition and improve efficiency in micro-credential platforms; also, it has the ability to verify every credential registered on the blockchain to ensure the validity and security of micro-credentials [17, 31]. Furthermore, although blockchain is a distributed database and several copies of the ledger are stored on different nodes, blockchain is not managed by a central authority, so it gives students full access to their credentials on micro-credential platforms [17, 76].

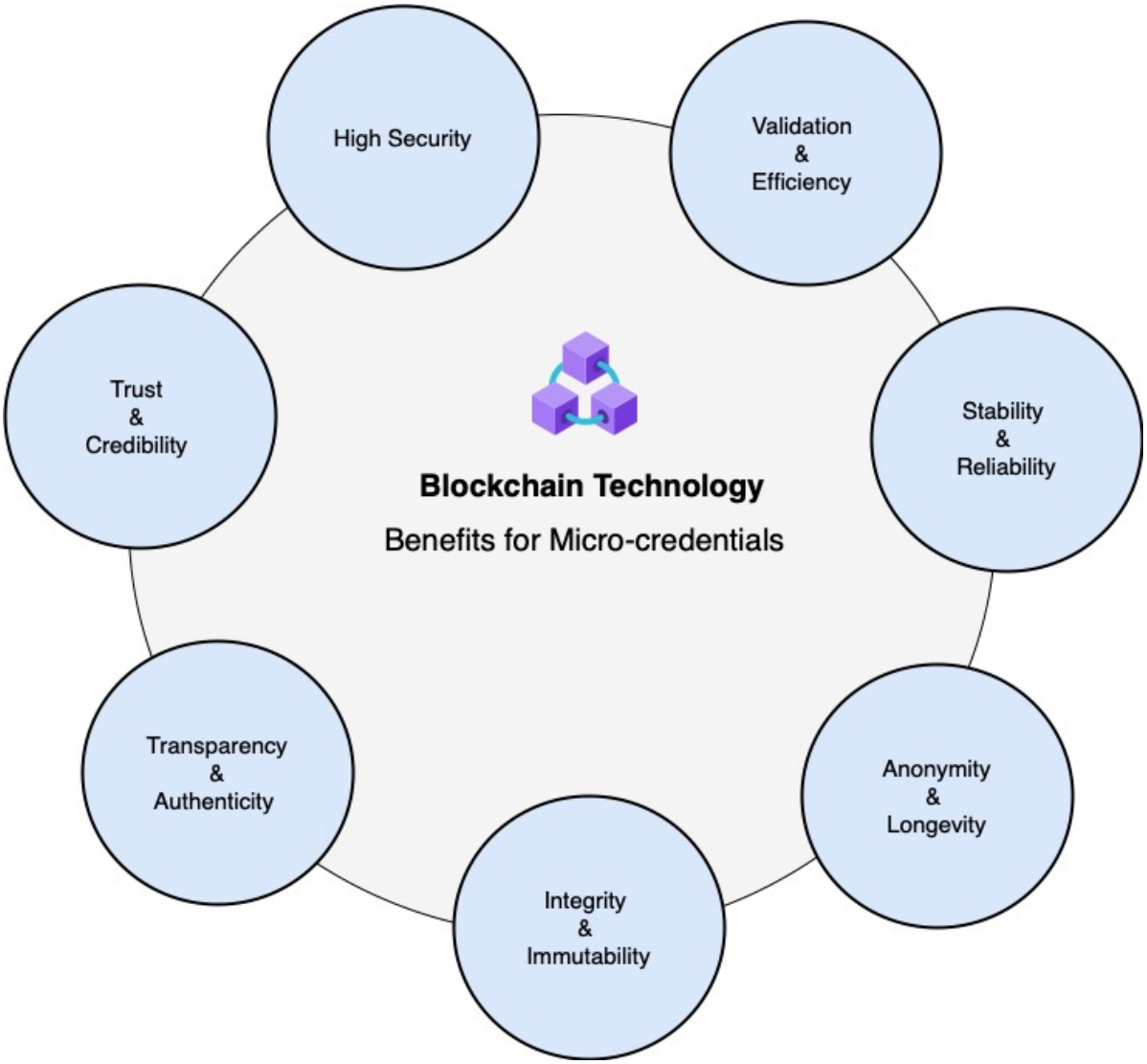

Figure 1.1: Benefits of blockchain for micro-credentials. (Alsobhi et al. [17])

1.3 Statement of the Problem

The number of international students applying to higher education institutions (HEIs) worldwide increases each year [3]. These students have made a decision to pursue higher education and they often need assistance regarding the management and evaluation of their previously completed micro-credentials. Many students are unfamiliar with academic degrees and micro-credentials during the application process. Therefore, they also require learning recommendations to support their learning journeys based on their micro-credentials and learning achievements [67]. Consequently, students encounter several challenges when pursuing higher education based on their micro-credentials,

detailed in the following.

There are multiple challenges associated with traditional methods of verifying credentials in higher education, like paper-based systems or centralized databases. The verification process is a manual check process and involves email exchanges with issuers or contacting issuer institutions [51]. When students send their credentials and academic documents to other HEIs, the institution's responsibility is to verify the authenticity of the credentials or certificates by contacting the original issuer and asking whether they were issued by them. Additionally, the original issuer might review their local or centralized databases of certificate records. However, if there is no database available for the original issuer, the credential or certificate will be verified using the paper-based method [20]. Therefore, the manual verification process is cumbersome, time-consuming, and inefficient, and it compromises overall credibility [51]. These challenges mainly involve authenticity and trust verification; unfortunately, when an efficient and reliable verification mechanism is absent, trust issues with the entire micro-credentialing process may result [58].

Additionally, one of the significant challenges for students is accessing their academic data online easily and in an unrestricted manner through their institution's platforms. These traditional e-learning platforms, typically used by most HEIs, often lack flexibility and accessibility [89]. Each HEI uses its own platform to store the students' data and academic records in specialized formats within restricted-access databases. As a result, students are unable to utilize their own data and have limited access to them [49]. Complicating matters, these centralized databases are controlled by third parties, which means students need permission to access their digital academic records, including credentials, certificates, and transcripts [89]. Furthermore, HEIs limit student control over their account along with restricted access by preventing them from accessing their academic records online once they graduate. In addition, there is no option for the students to share their credentials or academic records; they only have access to view or print it. Consequently, if a student loses their certificates or transcripts, they may have to go back to their home institution to obtain a replacement copy, which is time-consuming and can be expensive [89].

Generally, HEIs do not share their students' records with other institutions, which can prove problematic for students who want to transfer from one institution to another and need proof of previous coursework completion [86]. In this case, the students them-

selves are responsible for providing their academic documents to the other institutions. Moreover, it is particularly challenging for students who want to move to another country due to language barriers, script barriers, and administrative barriers [86]. Document exchange between institutions is typically difficult due to institutional autonomy and the lack of standardized formats for storing data. Because of these obstacles, the student's record will be duplicated in every institution with a different format, and the students may have to repeat some courses or complete unnecessary assessments, resulting in delays and wasted time [86]. Furthermore, the lack of standardized protocols and systems in HEIs in different countries complicates the sharing and transfer of students' academic records [86]. To learn effectively, students must own and control their digital academic records, determining who can access them and how they can share their credentials. Unfortunately, the existing e-learning platforms do not afford students adequate control over their credentials [49].

Security and privacy preservation are essential issues in e-learning areas that need to be addressed in the majority of education systems for student data integrity and protection against unauthorized access [89]. E-learning systems store sensitive information, including students' academic records and personal data. Moreover, many authenticated users, such as staff, administration, teachers, etc., can access the data that has been preserved on these systems to use, edit, review, and display. Subsequently, the students may desire anonymity to avoid revealing their personal information to other institutions while sharing their academic data with them [89]. For this reason, it is desirable that educational systems make student data anonymously searchable within previously agreed-upon parameters.
In most HEIs, students' academic records are stored in central repositories on institution servers. However, the centralized nature of these servers makes them prone to security issues, failures, and longer access times. Data security is at risk due to the presence of attackers on the network since they can potentially access sensitive information [14]. The inadequate security measures that the e-learning systems have implemented make them susceptible to unauthorized access [31]. Moreover, students may experience data loss and security breaches when sharing their educational data with other institutions through the system. In addition, the stored data is exposed to tampering, fraud, and privacy breaches [14]. For instance, in 2020, the records of 20,000 students at Sias University in Zhengzhou were leaked [62]. In 2022, the hacking of the contact details for 47,000 students at Deakin University in Australia exposed student IDs, names, phone numbers,

and email addresses [34].

In addition, there is a lack of an intelligent mechanism that allows students to select the right major based on their micro-credentials and learning achievements. There is a need to assist students regarding the appropriate selection of majors that are relevant to their completed micro-credentials. Choosing the right major is a crucial decision that profoundly affects a student's career path in the future. Furthermore, several factors influence this decision, including limited knowledge of the major, relying on online searches, recommendations from friends, parents' opinions, and family pressures, etc. [16]. There can be serious consequences for both the HEI and the student if a student selects an inappropriate major. As an example, it may negatively impact students' career prospects, resulting in decreased interest, motivation, academic performance, and difficulty finding a suitable job [32]. In addition, the decision to change a major or to not complete a degree may also result in students wasting valuable time and resources, which can adversely impact their future academic and professional careers [32]. The National Centre for Education Statistics (NCES) indicated that approximately 80% of university students decided to change their majors at least once during their study in 2020 [32]. This suggests that many new university students lack the experience that they need to make informed decisions about their academic majors.

The lack of a unified platform that aggregates and presents all action plans is a significant challenge. This challenge makes it difficult for students to manage their academic goals effectively [48]. This problem occurs when students apply to several HEIs and receive an action plan from each of them. To make informed decisions regarding their academic path, students need to be able to access and view their action plans in one accessible place. While there are existing educational platforms, none of these platforms address the essential need of aggregating action plans from multiple HEIs. Consequently, as there is currently no platform that aggregates all students' action plans into one easily accessible view, the students have to navigate several systems and interfaces to access their action plans, which is difficult, resulting in confusion, wasted time, and possible errors.

Consequently, choosing an appropriate action plan from multiple options on the basis of various criteria is also another issue for students. This issue occurs because it may be difficult for students to obtain comprehensive information about each action plan, and

every criterion has its own significance and may impact the final decision [11]. Decision-making is a complicated process, requiring students to assess and weigh different factors before making a well-informed decision. Further complicating this decision-making process is the lack of an intelligent and simplified process for evaluating and comparing action plans effectively based on these various criteria [11]. The absence of an effective framework or tool to support students' decision-making processes may result in them feeling confused, overwhelmed, or lacking in confidence during the selection process.

1.4 Motivation of the Thesis

According to a recent qualitative research study, there is now a barrier to the wider adoption of blockchain due to the general lack of awareness of employing blockchain technology in the context of micro-credentials [17, 38]. Recently, the number of studies on the application of micro-credentials on blockchain in higher education has been increasing, but no study has been conducted on this research subject. Furthermore, in the higher education sector, there is a lack of intelligent approaches and applications to reliably manage micro-credentials [12, 17]. HEIs are still in the early phases of managing micro-credentials based on blockchain technology [17, 76].

There is a need for HEIs to develop an innovative and trustworthy approach to securely store micro-credentials and to share these micro-credentials with other stakeholders (such as but not limited to HEIs). According to [32, 85], there is an urgent need for intelligent and reliable approaches to provide recommendations for learning pathways for students. Based on the micro-credentials and a student's learning preferences, such as a particular degree, major, course, etc., a personalized action plan can be generated by HEIs. Managing, aggregating, sharing, preserving, and storing micro-credentials in a decentralized environment is crucial for both students and HEIs [17]. Therefore, developing a decentralized higher education micro-credential platform will serve as a trustworthy and intelligent mechanism to manage and store the student's completed micro-credentials [17, 49]. It is important that this platform provides support to students by allowing them to share micro-credentials in a privacy-aware manner [31]. Furthermore, the micro-credential platform should be able to generate learning recommendations for majors and action plans for the students [17].

Given the importance of using blockchain to manage micro-credentials in HEIs and

the challenge of developing a decentralized micro-credential platform, previous studies [30, 58, 89] have proposed different credential platforms in the higher education sector. However, their approaches do not focus on the possibility of the acquired micro-credentials being used to complete a specific degree in the future with a suitable major [17].

To address the limitations and issues explained previously in Section 1.3, we first need to identify the main requirements, from the student's perspective, that need to be met in providing an optimal blockchain-based micro-credential platform. We have identified four important requirements as follows. In the future the innovative micro-credential platform should be able to do the following [17]:

1. store, verify, and share micro-credentials in a privacy-preserving manner.
2. enable students to access their micro-credentials anywhere and at any time without a central authority.
3. collect all the provided action plans from multiple HEIs and display them to the students in a single view so they can select a suitable one based on their preferences.
4. generate personalized learning recommendations as requested for action plans and majors, based on the students' micro-credentials.

1.5 Objectives of the Thesis

This thesis addresses some existing issues associated with managing micro-credentials in higher education. Specifically, it proposes an effective methodology for developing an intelligent and reliable platform dedicated to higher-education micro-credentials that meets the needs of both students and HEIs. Through the accomplishment of this main objective, this study contributes to the advancement of micro-credentialing systems and improving the management efficiency and effectiveness of micro-credentials in higher education. We summarize the main objectives of this research based on the previously identified requirements:

1. This thesis develops a reliable blockchain-based framework for managing and verifying students' micro-credentials, ensuring the integrity and authenticity of

their academic achievements. The framework leverages blockchain's inherent security and immutability to offer a trusted and tamper-proof micro-credential management platform.

2. This thesis designs a privacy-preserving solution that enables students to keep their identities secure while sharing their academic profiles with other institutions on the blockchain. This solution ensures the confidentiality of students' identities, while also ensuring that micro-credentials can still be verified and recognized more easily.

3. This thesis develops a recommender system that provides students with learning recommendations for the most suitable major that aligns with their micro-credentials and academic achievement. Using machine learning techniques and data analytics, the system empowers students to make informed educational decisions regarding their academic pursuits.

4. This thesis provides a methodology for students by which they can access and view all their action plans received from several HEIs in one location. By using this approach, action plans can now be easily managed and tracked, giving students a comprehensive understanding of what is available to them.

5. This thesis proposes an intelligent methodology by which students can predict the best action plan based on multiple criteria to make informed choices regarding their learning aspirations and align their choices with their long-term goals by considering multiple criteria.

1.6 Scope of the Thesis

Our main research objective is to develop a blockchain-based micro-credential platform that can assist HEIs and students in verifying, managing, maintaining, and sharing micro-credentials.

During this study, innovative approaches for increasing the credibility and reliability of micro-credentials across the higher education ecosystem are explored, as well as the challenges and opportunities associated with managing micro-credentials over a lifetime. As part of its focus on platform development, this thesis addresses key issues concerning

micro-credential provenance, verification, security, and interoperability.

Using emerging technologies, such as blockchain, artificial intelligence, or privacy preserving, this thesis examines the potential benefits of developing a micro-credentialing system that enhances transparency and trustworthiness. In addition, this thesis explores the relationship between students' prior educational achievements and their future education qualifications to provide insights and learning recommendations.

Overall, the major aim of this thesis is focused on providing a comprehensive methodology that can be used to manage, verify, share and store micro-credentials using blockchain technology, as well as providing personalized recommendations for students based on their micro-credentials.

1.7 Contributions of the Thesis

This thesis proposes a trustworthy and intelligent blockchain platform for managing higher-education students' micro-credentials. This section discusses the thesis contributions, which are classified into scientific and social contributions.

1.7.1 Scientific contributions

This thesis makes the following scientific significance to the existing literature:

1. This is the first research that proposes a privacy-preserving method to ensure the students' anonymity while sharing their academic profiles with HEIs.

2. This is the first research that develops a recommender system to assist students in selecting a suitable major based on their micro-credentials.

3. This is the first research that proposes an intelligent mechanism to assist students in selecting a suitable action plan based on their preferred parameters.

4. This is the first research that provides learning recommendations to assist students in completing their preferred degree based on their micro-credentials.

1.7.2 Social contributions

1. This research can help in building academic profiles, including skills, qualifications, experiences, and completed micro-credentials from multiple HEIs online in a distributed, intelligent, and reliable environment for students.

2. This research will help in aggregating and converting students' micro-credentials into a specific academic degree to pursue their learning journey. It also provides personalized learning recommendations for students based on their verified micro-credentials.

3. This research in the future will benefit employers as potential users of the system as they will be able to validate the data provided by an employee for a specific job.

1.8 Plan of the Thesis

The main goal of this thesis is to provide a complete methodology for developing an intelligent blockchain platform design to manage micro-credentials for higher-education students. To achieve this goal, various techniques, machine-learning models, and artificial intelligence algorithms were used. This thesis is structured into eight chapters as shown in Figure 1.2. This section provides the following overview of each chapter:

- **Chapter 2:** This chapter provides a systematic literature review to review and analyze the existing blockchain-based higher education micro-credentialing platforms in the current literature. In this chapter, we identify and review the shortcomings in the existing literature that have not yet been adequately addressed and resolved. To contribute to the field, we address the gaps identified in this thesis.

- **Chapter 3:** This chapter defines each of the gaps that have been identified in the previous chapter and we address them in this thesis. In addition, this chapter presents definitions of the terms used in this thesis to define the issues that will be addressed. Furthermore, this chapter formulates research questions based on the identified research gaps, which are then also used to devise the research objectives.

- **Chapter 4:** This chapter defines the main research methodology chosen as the most pertinent to this research to address the research gaps. The design science research approach is the methodology chosen for this research. Additionally, an overview of a proposed solution to each of the identified gaps is presented in

Chapter 3. This chapter includes references to the chapters that contain detailed solutions to the research issues identified. Additionally, some terminologies are defined conceptually in this chapter.

- **Chapter 5:** This chapter describes in detail the development of the intelligent blockchain for managing micro-credentials (IBMM) platform. This is a higher-education micro-credentialing platform that is designed and built using the Hyperledger blockchain. It is an intelligent and reliable platform for higher education students used to store, verify, and manage micro-credentials. The IBMM platform contains three layers, each of which is presented and explained in detail. In addition, this chapter presents the privacy-preserving methodology by which a student can share their profiles and micro-credentials securely and privately between HEIs via the IBMM platform.

- **Chapter 6:** This chapter provides a detailed description of the proposed solution for recommending the most suitable major for students. It focuses on developing a recommender system that uses students' micro-credentials to predict an appropriate major for each student. To design this recommender system, three machine-learning models are used, and each of these three models is discussed in detail.

- **Chapter 7:** This chapter introduces and explains the methodology of collecting students' action plans to enable the students to easily access and view them via the IBMM platform. These action plans are generated based on the students' micro-credentials which are received from several HEIs. Furthermore, this chapter presents a multi-criteria decision-making methodology by which used to help the students in choosing the most optimal action plan based on their selected criteria. We utilized one deep-learning model and two machine-learning models and presented them in detail in this chapter.

- **Chapter 8:** This chapter is the final chapter of this thesis, and it offers a brief summary of the major contributions and achievements made through this research. Moreover, it outlines possible directions for future work that can extend and enhance the findings contained within this dissertation.

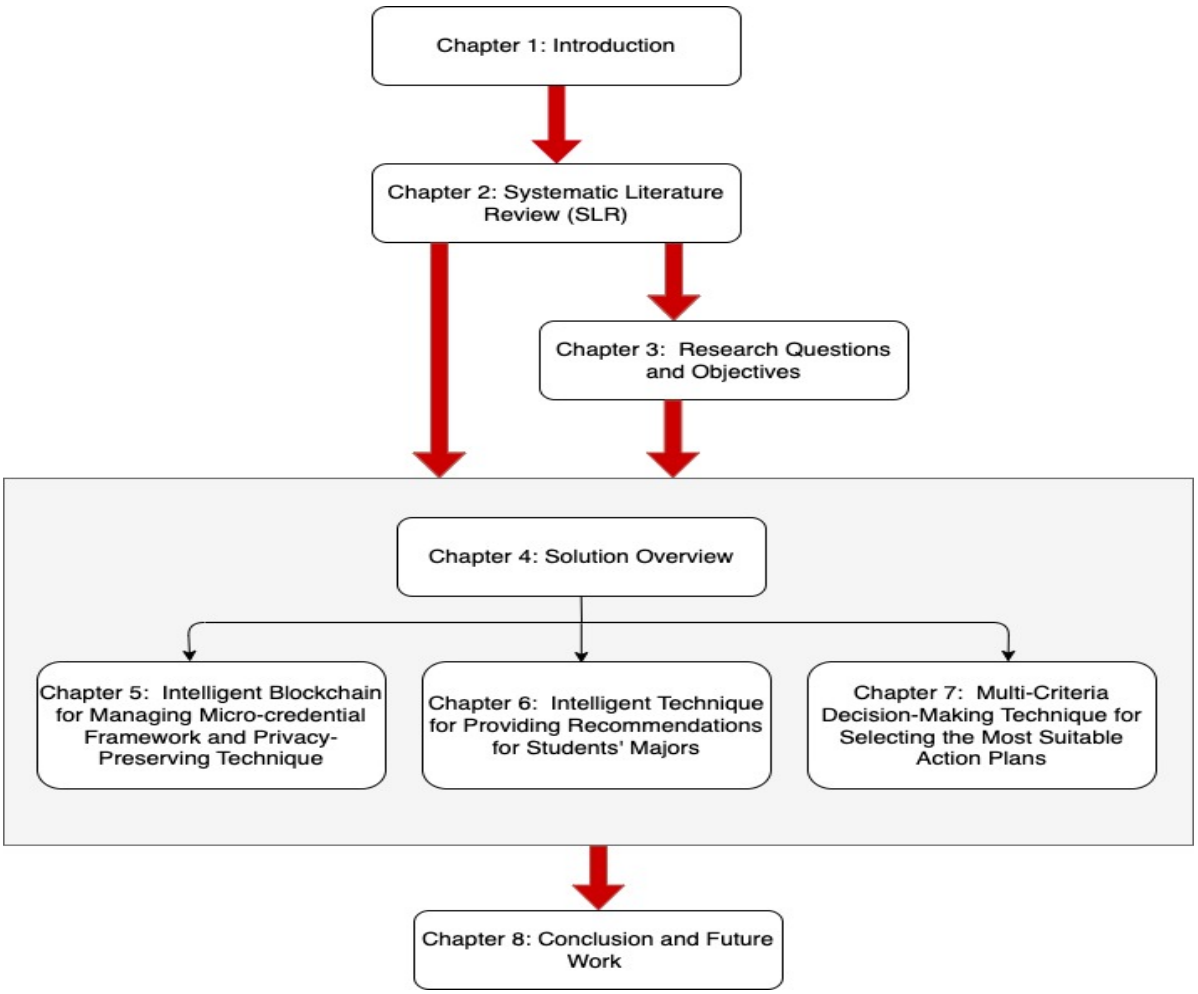

Figure 1.2: The structure of this thesis

1.9 Conclusion

In conclusion, this chapter presented an introduction to our thesis, which is focused on developing an intelligent and trustworthy blockchain platform for managing micro-credentials in the higher education sector. It provided a concise background description of micro-credentials, blockchain technology, and the concept of blockchain-based micro-credentials. Furthermore, the problem statement, research objectives, and scope, research motivation, research contributions, and thesis plan were presented in this chapter.
The next chapter presents a systematic literature review (SLR) process to identify the research issues that have not been addressed by previous research and need to be addressed in this thesis.

CHAPTER 2

A SYSTEMATIC LITERATURE REVIEW

2.1 Introduction

This chapter provides a detailed overview of the state-of-the-art in the field of managing micro-credentials using blockchain technology. The primary motive of this chapter is to review the existing literature which has been published over the past seven years, from 2016 to 2023. We start by conducting a systematic literature review (SLR) to retrieve the relevant studies to present an innovative and timely contribution to the literature on blockchain-based micro-credential platforms in the higher education sector. Additionally, we conducted an analysis of the existing literature to identify the research gaps. This review offers insight into the micro-credential platforms that have been proposed for HEIs over recent years. Then, we classify the existing platforms in each of the reviewed studies into two groups, namely intelligent platforms for managing micro-credentials (IPMM) and platforms for managing micro-credentials (PMM).

The contents of this chapter have been published in the Knowledge-Based Systems journal, which is currently ranked in the top quartile of journals (JCR Q1, IF impact factor 8.8). The contents of this SLR are available at the following link: `https://www.sciencedirect.com/science/article/abs/pii/S095070512201334X`.

This chapter is organized as follows: Section 2.2 introduces the SLR and discusses the process adopted to shortlist the articles chosen for this SLR based on the inclusion and

exclusion criteria used for the search. Section 2.3 analyses the final 15 studies which are divided into two categories, namely IPMM and PMM. Section 2.4 discusses the research issues found in the relevant studies. Section 2.5 concludes this chapter.

2.2 Systematic Literature Review

A systematic literature review (SLR) is a useful technique for reviewing and analyzing previous works to gain a clear insight into the management of micro-credentials. The main reasons for using this approach are to find the research gaps, address the research questions posed in the existing articles, and evaluate all the available studies that have been published on this research topic. A review is crucial to give a current overview of the subject and to support evidence-based practice. To provide a thorough evaluation of the literature on managing the micro-credentials examined in scholarly journals and conference proceedings, our research uses a pragmatic technique. Additionally, the articles should focus specifically on blockchain-based micro-credential platforms in the higher education section as there are a lot of studies that discuss the micro-credentials concept in general however, there has been no systematic review conducted to date on this research subject. In this SLR, all the relevant studies were reviewed and critically evaluated. The steps involved in conducting an SLR process are as follows:

2.2.1 Step 1: Data source selection and search process

To extract the relevant articles, this stage involves identifying the keywords, search terms, and data sources or databases that can assist.

- The scientific online databases and the search engine platform that were selected and used in this literature review are as follows:

    1. IEEE Xplore Digital Library (`www.ieexplore.ieee.org/Xplore`).
    2. Springer Link (`https://link.springer.com`
    3. ProQuest Science and Technology (`www.proquest.com`).
    4. Elsevier ScienceDirect (`www.sciencedirect.com`).
    5. Scopus (`www.scopus.com/`).
    6. Web of Science (`https://www.webofscience.com`)
    7. Google Scholar (`https://scholar.google.com`).

These carefully chosen electronic databases offer adequate coverage of the literature pertinent to this SLR analysis. Google Scholar is another well-known database that may be able to identify more relevant papers than the other scientific databases.

- The following search categories and keywords were used in this SLR to search for and identify the related articles:

  1. **Blockchain:** distributed ledger.
  2. **Micro-credentials:** digital credentials, digital badges, micro-certification, micro-learning.
  3. **Higher Education:** higher education institution, university, college.

  We employed a search technique to create a database of the literature to identify the most similar research. We utilized a variety of search terms including (("blockchain" OR "distributed ledger") AND ("micro-credentials" OR "micro-credentials" OR "micro-credential" OR "micro-credential" OR "digital credential" OR "digital credentials" OR "digital badges" OR "digital badge" OR "micro-certification" OR "micro certification" OR "micro-certifications" OR "micro certifications" OR "micro-learning" OR "micro-learning") AND ("higher education institutions" OR "university" OR "college")). We used the Boolean operator "AND" to combine the keywords from different search categories and the Boolean operator "OR" when using many keywords from the same category. We used a different query string for each database since each defines its own search syntax and we retrieved 322 articles.

- The search period was between 2016-2023. We used the search terms with each database to find relevant journal and conference papers published during this period. The date of the last search was August 2023.

2.2.2 Step 2: Inclusion and exclusion criteria

In this step, the 322 papers that were retrieved in the previous step were evaluated in terms of the inclusion and exclusion criteria to determine whether or not they would be included in the SLR. To reduce the number of studies that were retrieved, we applied inclusion and exclusion criteria to the search output of the prior step. After removing irrelevant and duplicated studies, 177 papers were retrieved based on the inclusion and exclusion filtration criteria as follows:

1. Inclusion Criteria:
    - The study must discuss the management of micro-credentials for higher education students.
    - The paper must be written in the English language.
2. Exclusion Criteria:
    - A paper that is a workshop paper, an article from a magazine or newspaper, a thesis, or a poster session.
    - A paper that is a duplicate article or a survey article.

2.2.3 Step 3: Study selection process

Four filtration phases were followed in this step, as shown in Table 2.1:

- The first stage was based on all the search terms, returning 322 articles from the online search. Of these, 107 were retrieved from the six scientific databases, and 215 were retrieved from Google Scholar. The number of articles was reduced to 177 after the inclusion and exclusion criteria were applied and the duplicate papers were removed. Therefore, 145 articles were removed from the selection process based on the inclusion criteria.
- The second stage was based on the study title, so after screening the title, the number of the retrieved articles was reduced to 80, and 97 studies were excluded. However, it is challenging to make a decision to include or exclude a study based only on the title, therefore, we implemented the third stage.
- The third stage was based on each paper's abstract. After carefully reading and assessing each of the 80 abstracts to determine whether the study was relevant to this research, the number of articles was reduced to 48, and 32 papers were excluded.
- The fourth stage involved reading and analyzing the full texts of the 48 articles to select the studies that were the most relevant to this research, hence 30 studies were removed. As we are only investigating studies that discuss the management of micro-credentials in the higher education sector, 18 articles were selected for further analysis. Table 2.1 shows the number of articles that were retrieved at each filtration stage.

Database	Number of papers based on keywords	Number of papers based on titles	Number of papers based on abstracts	Final number of papers based on full text
IEEE Xplore	10	8	6	5
Springer Link	43	7	5	1
ProQuest	37	6	3	1
ScienceDirect	4	2	1	1
Scopus	8	5	3	2
WOS	5	2	1	0
Google Scholar	215	50	29	8
Total	322	80	48	18

Table 2.1: Number of papers selected at each stage

2.2.4 Step 4: Quality assessment and data extraction and synthesis

In this step, each paper was evaluated to determine whether it satisfies the quality standards, and the 18 papers were analyzed in detail to ensure that only the most relevant papers were included in this SLR.
We defined some quality criteria and then critically evaluated all 18 articles against the following four quality assessment criteria to make sure that the selection process was unbiased:

QA1: Does the study deal with micro-credentials at the higher education level?

QA2: Does the study deal with blockchain technology?

QA3: Does the study introduce a proper framework to address its aim?

QA4: Is the proposed methodology validated by proof of concept or implementation?

This SLR includes papers that have at least three "yes" answers to each of the four quality assessment criteria. Table 2.2 presents the evaluation of the 18 papers based on the quality assessment criteria. The final set of included studies was selected based on the various evaluation criteria to ensure their relevance to this research topic. Thus, if the study met these criteria, it was deemed to be suitable for this SLR. As shown in Table 2.2, only 15 papers met the criteria and were included in this SLR. Figure 2.1 illustrates the selection procedure for the articles that were included in each stage of this SLR.

We extracted the most relevant data from every paper based on the research questions. Every selected paper was analyzed according to its scope, topic area, paper type, the study's aims, author's information, language, and summary of its research questions and answers. After this analysis, all the data extracted from the selected studies were synthesized, which allowed us to classify the final 15 studies into two categories (IPMM and PMM). As shown in Table 2.3, 11 studies did not use any intelligent techniques, so they were classified as PMM and 4 studies used intelligent techniques, so they were classified as IPMM. The following section summarizes and discusses the shortlisted papers to analyze each existing study in both the IPMM and the PMM categories.

Research Paper	**Quality Assessment Questions**			
	QA1	**QA2**	**QA3**	**QA4**
Arenas and Fernandez [20]	Yes	Yes	Yes	Yes
Choi et al. [30]	Yes	Yes	Yes	Yes
Kishore et al. [58]	Yes	Yes	Yes	Yes
Lim et al. [63]	Yes	Yes	No	Yes
Turkanovic et al. [89]	Yes	Yes	Yes	Yes
Mikroyannidis et al. [71]	Yes	Yes	Yes	Yes
Mikroyannidis et al. [70]	Yes	Yes	Yes	Yes
Mikroyannidis et al. [69]	Yes	Yes	Yes	Yes
Ghasia et al. [40]	Yes	No	No	Yes
Jirgensons and Kapenieks [51]	Yes	Yes	No	No
Chukowry et al. [31]	Yes	Yes	Yes	Yes
Ahmat et al. [12]	Yes	No	Yes	No
Mainetti et al. [65]	Yes	Yes	Yes	Yes
Terzi et al. [88]	Yes	Yes	Yes	Yes
Ghonim and Corpuz [41]	Yes	Yes	Yes	Yes
Kumaresh [60]	Yes	Yes	Yes	Yes
Srivastava et al. [86]	Yes	Yes	Yes	Yes
Alam et al. [15]	Yes	Yes	Yes	No

Table 2.2: Assessment of the papers against the quality criteria questions

2.3 Analysis of Shortlisted Papers in the IPMM and PMM Categories

IPMM is an AI-supported platform for managing micro-credentials based on the content of the certificate, i.e., the topic undertaken, the major undertaken, job prospects, etc.

Research Paper	Title	Category
Mikroyannidis et al. [71]	A Case Study on the Decentralisation of Lifelong Learning Using Blockchain Technology	IPMM
Mikroyannidis et al. [70]	Supporting Lifelong Learning with Smart Blockchain Badges	IPMM
Mikroyannidis et al. [69]	Smart Blockchain Badges for Data Science Education	IPMM
Mainetti et al. [65]	Digital Brick: Enhancing the Student Experience Using Blockchain, Open Badges and Recommendations	IPMM
Arenas and Fernandez [20]	CredenceLedger: A Permissioned Blockchain for Verifiable Academic Credentials	PMM
Choi et al. [30]	Blockchain-Based Badge Award with Existence Proof	PMM
Kishore et al. [58]	Blockchain-Based Micro-credentials: Design, Implementation, Evaluation and Adoption	PMM
Lim et al. [63]	Developing a Framework for the University-Wide Implementation of Micro-Credentials and Digital Badges: A Case Study from a Malaysian Private University	PMM
Turkanovic et al. [89]	EduCTX: A Blockchain-Based Higher Education Credit Intelligent platform	PMM
Chukowry et al. [31]	The future of continuous learning,ÄìDigital badge and micro-credentialing system using blockchain	PMM
Terzi et al. [88]	A Life-Long Learning Education Passport Powered by Blockchain Technology and Verifiable Digital Credentials: The BlockAdemiC Project	PMM
Ghonim and Corpuz [41]	Moving Toward a Digital Competency-based Approach in Applied Education: Developing a System Supported by Blockchain to Enhance Competency-Based Credentials	PMM
Kumaresh [60]	Academic Blockchain: An Application of Blockchain Technology in Education System	PMM
Srivastava et al. [86]	A Distributed Credit Transfer Educational Framework based on Blockchain	PMM
Alam et al. [15]	A Blockchain-based framework for secure Educational Credentials	PMM

Table 2.3: Categorization of articles as either IPMM or PMM

It also includes personalized recommendations that use machine learning or artificial intelligence (AI) algorithms to carry out intelligent tasks, such as providing recommendations to students in relation to courses, jobs, or majors and making predictions relating to students' selections as well as storing and managing micro-credentials. For example, Digital Brick is an intelligent platform for managing micro-credentials using artificial intelligence methods to provide personalized recommendations for course materials and learning paths for students [65].

PMM differs from IPMM as it is a platform that does not use machine learning or AI algorithms to carry out intelligence tasks and provide learning recommendations or make predictions. This category of platform only offers a mechanism for storing and managing micro-credentials. For example, EduCTX is a platform for managing and

storing micro-credentials, but it does not make recommendations or predictions for students [89].

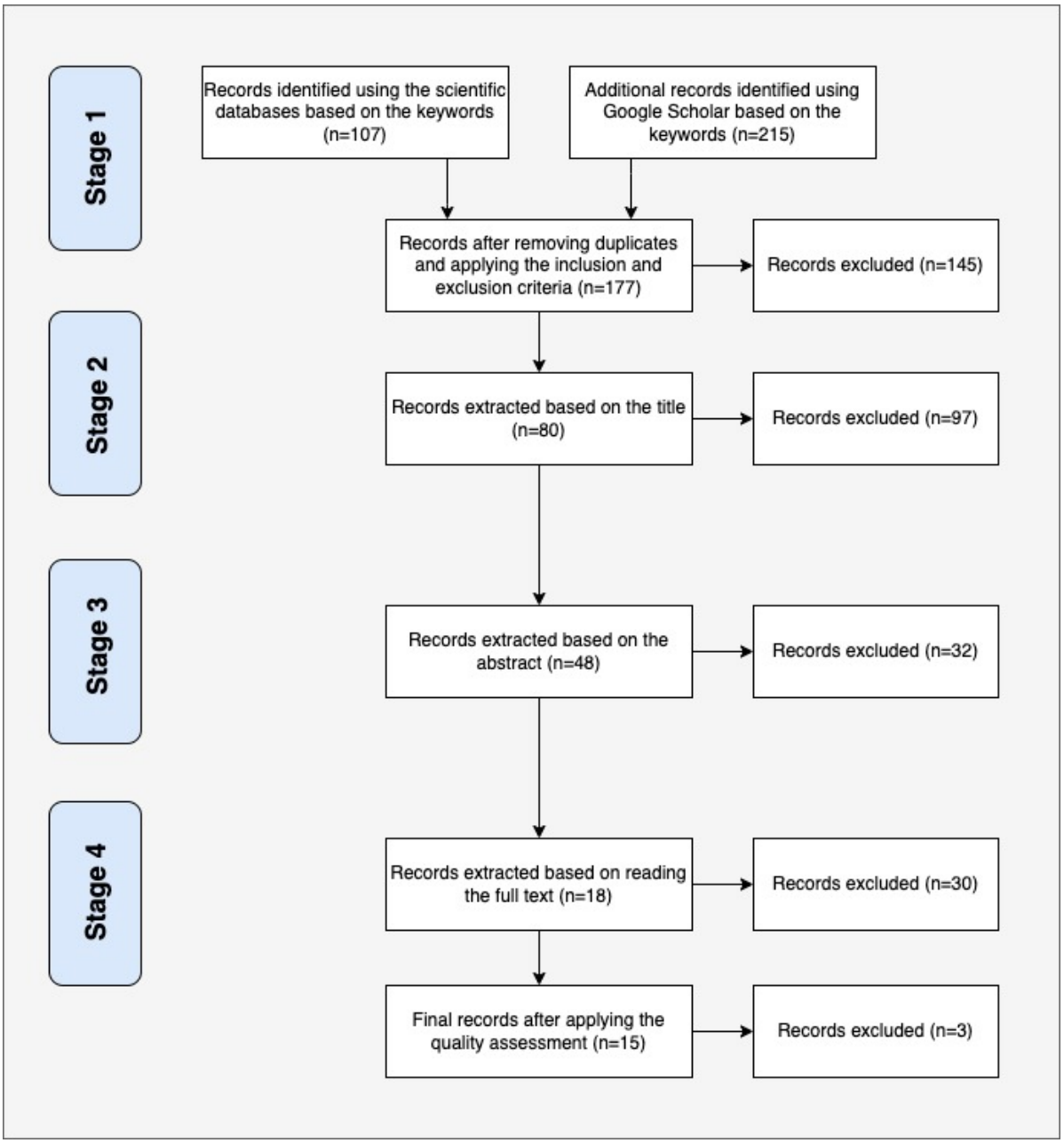

Figure 2.1: Selection process of the SLR

2.3.1 Intelligent platform for managing micro-credentials (IPMM)

As shown in Table 2.3, only four of the proposed micro-credential platforms in the existing literature carry out intelligent tasks. In this study, we define an intelligent platform as any platform that applies an artificial intelligence (AI) technique. Intelligent learning platforms have many advantages for students, such as offering personalized recommendations for a job or course, offering reliable data about the students and their educational data, and making appropriate recommendations for students during their education journey.

Mikroyannidis et al. [69] applied smart blockchain badges to enhance the certification of data science by providing a powerful framework built on blockchain. This system assists students who want to improve their careers in the field of data science by providing job recommendations that are compatible with their skills and educational qualifications. A smart badge has dynamic features that can be used to make recommendations for a job or course. The European Data Science Academy project developed an interactive dashboard to offer automated tools to build personalized learning pathways that help students reach their learning and career objectives [69]. Students who study a variety of data science disciplines can receive badges/micro-credentials by successfully finishing a course in its entirety or in part and these badges are recorded on the blockchain. When the students earn more badges, they begin to receive recommendations for the most recent job openings that meet their qualifications. They also receive recommendations for additional courses so they can acquire the additional experience needed for a specific job [69].

Moreover, Mikroyannidis et al. [68] described a new ecosystem called a student-centered approach which puts students at the center of the learning process and its associated data. The authors also discuss how this new model affects various aspects of lifelong learning [68]. The Ethereum Blockchain platform is used to implement the core components of this student-centered ecosystem with a focus on how e-portfolios, accreditation, and tutoring can be developed, as well as the different benefits this evolution can provide to lifelong learners[68].

Later, Mikroyannidis et al. [71] proposed a decentralized solution using blockchain that allows students to devise a better learning plan depending on their intended job path which gives them complete control over their education data and procedures. A reputational ecosystem was developed to allow students to rate courses, online materials, and professors in terms of how easy they are to understand and other factors relevant to their unique learning objectives. Also, students can give each other ratings on a variety of attributes. Furthermore, the authors discussed several approaches to the semantic blockchain and how these approaches can be applied to e-learning [71]. The semantic blockchain provides a way to combine all of an individual's obtained learning skills and credentials to produce a comprehensive image of their lifelong learning [71].
In this research, the authors conducted a pilot case study on lifelong learning based on the semantic blockchain that attempts to apply a decentralization technique to manage various requirements such as integrity, accessibility, and confidentiality [71]. The aim of the pilot study is to provide job and course recommendations and unchangeable learning credentials to lifelong learners to help them reach their learning and career goals. This is to support lifelong learning using blockchain technology and combining smart badges and personalized recommendations [71]. The authors report in this study that they have completed the first phase in relation to requirements elicitation and will embark on the second phase of designing, installing, and testing this pilot case study.

For the second phase, Mikroyannidis et al. [70] proposed an initial web-based prototype to implement, deploy, and evaluate the lifelong learning pilot study. Personalized recommendations are also used as an intelligent process to assist lifelong learners in achieving their personal and career learning objectives. Using blockchain technology enables lifelong learning to become decentralized and provides lifelong learners with a transparent and unchangeable educational framework in the format of smart badges to assist them in reaching their learning objectives and career pathways [67]. Therefore, this decentralized solution makes it possible to store, share, and verify educational credentials (formal and informal) and then offers personalized recommendations about careers and what to study next, based on the student's previously acquired credentials [67]. When all the datasets containing job offers and their related skills are stored in smart contracts on the Ethereum blockchain, job offers can be matched to the student's skills[70].

Mainetti et al. [65] designed a novel e-learning system architecture called Digital Brick to improve the experience of students when receiving official certifications of their competencies. This system is built on the shareable content object reference model (SCORM) learning management system that offers all stakeholders in the learning field access to a certification system and makes use of blockchain and open badge technologies. The main goal of this research is to provide students with accessible and adaptable online environments so they can select and complete courses and receive formal learning certifications. To achieve this goal, the authors proposed an intelligent platform that innovates how students can acquire and share the official certifications they receive to improve the students' experience [65].
Moreover, the authors used digital badges/micro-credentials to issue formal certifications and blockchain technology to increase the security, openness, and transparency of badge sharing among stakeholders. A private Ethereum blockchain was used as a network and smart contracts were deployed to represent digital badges that indicate the student's achievements. The authors also developed a novel recommendation system based on machine learning algorithms to recommend the course materials and learning paths that are best suited to the student's learning strategies to obtain formal digital badges and certifications [65]. A hybrid system of collaborative filtering with content-based filtering was used to develop the recommendation system. Finally, to evaluate the system and obtain the results, they used a laboratory case study that included all the features of the system architecture. The results show that better transaction throughput and latency were attained for the certification system and better prediction accuracy was attained for the recommendation system [65].

.

2.3.2 Platform for managing micro-credentials (PMM)

The other platforms that are presented in the existing studies for managing micro-credentials offer mechanisms to manage, verfiy, and store micro-credentials, but they do not perform tasks intelligently. As shown in Table 2.3, there are 11 proposed platforms in the reviewed literature that have been classified under the PMM category.

Turkanovic et al. [89] proposed EduCTX, a distributed blockchain-based micro-credential for higher education and the European Credit Transfer and Accumulation System (ECTS), which is a global grading system that can manage, assign, and process ECTX tokens as a digital academic micro-credential for every student and HEI. This

platform manages and processes micro-credentials based on blockchain technology and provides a solution to a number of difficulties, including language, administrative barriers, and unemployment. Additionally, this technology transforms academic credentials into a worldwide, easier, more omnipresent format [89]. Students will benefit from having access to all their previously completed courses in one place, and HEIs will have access to this data as well. After obtaining the approval of a student, multiple HEIs can verify the submitted micro-credentials. The first version of the EduCTX prototype was built on the Ark blockchain technology [89], and the second version was developed based on the Ethereum blockchain and used smart contracts to guarantee security, privacy, trustworthiness, and speed [49].

Lim et al. [63] discussed several micro-credentialing implementation possibilities for undergraduate programs at Taylor's University. The micro-credentials can be executed using TIMeS, a learning management system (LMS) as the basic platform, and can be stored and verified using blockchain technology. The authors described the student learning journey through the micro-credential ecosystem in each phase [63]. A student must meet the requirements for micro-credentials in order to receive them. Once the required program has been completed by the student, digital badges are issued automatically as a result of the integration of the developed micro-credential platform with the LMS. This eco-system enables students to share their digital badges on social media and professional networks, as well as to use them to demonstrate their achievements to potential employers [63]. In addition, it is a very helpful platform for students to earn micro-credentials from undergraduate programs at Malaysian universities [63].

Kishore et al. [58] designed, implemented, and evaluated a system based on blockchain to manage micro-credentials that operate independently and are housed in the executive education programme of a business school. This system is based on MIT's Blockcerts project, and the credentials are securely verified using blockchain technology [58]. The evaluation of this system's implementation is based on understanding user perceptions (the certificate issuer and recipient). The authors used the design science research methodology (DSRM) to allow users to use this system for a long time and to make the credential generation process easier. They used cert-manager as an online form that the issuer completes with information including the title of the certificate, a description of the certificate, the logo on the certificate, and a list of receivers in a file [58]. This information is compiled and sent to cert-tools, a module that creates certificates for each

student, after which the cert-issuer generates a certificate hash for verification, and the cert-viewer helps to display and verify certificates online. In terms of the evaluation process, the authors used a qualitative approach, including interviews with students who had earned micro-credentials and issuers who created the credentials for the students [58]. This work looks at how a micro-credentialing system is implemented, with a special focus on user impressions.

Choi et al. [30] used blockchain technology to implement a digital badge-awarding platform for the education sector. This platform was used across many platforms to earn, issue, exchange, and award badges that are compatible with Open Badges of the IMS Global Learning Consortium [30]. To keep the information safe, these badges were stored, authenticated, and issued in a blockchain and can be displayed online to interested third parties to demonstrate the student's skills and knowledge. The authors employed two platforms: the Badgr platform for issuing digital badges, and the Blockcert platform for managing digital badges via blockchain [30]. The Badgr platform creates a digital badge with a picture and metadata, where the image represents the accomplishment and the metadata reflects the details of the accomplishment, and then it is published in two formats: text and URL (JSON) and image (PNG) [30]. With this platform, all students are able to participate in lifelong learning and online distance education.
This research is applicable to micro-learning units in training courses and online education courses. When a student completes a micro-learning unit, they receive a digital badge. The digital badges of the suitable micro-learning units are issued when the requirements are satisfied, and these badges are used to issue certificates for courses or degrees [30]. Every student has an e-portfolio in which they can save and manage their badges, as well as manage their careers. A student can grant organizations or individuals permission to access their e-portfolio [30]. This paper offers a blockchain-based badge awarding system for managing micro-learning unit digital badges.

Chukowry et al. [31] proposed a web-based micro-credentialing system to assist students in obtaining new skills or improving their skills in a shorter time and in a simpler and more adaptable way. This system was built based on the Ethereum blockchain which is a trustworthy, decentralized, and immutable system that has gained students' trust and performs significantly better than conventional e-Learning platforms [31]. The proposed micro-credentialing system includes quizzes and digital badges that store the badge image and firebase for examination, registration, and storing courses [31].

A micro-credentialing system has many features, for example, it is more practical which can help a student save time and cost, they can complete more courses in the same time frame of one university course, and they can easily choose their preferred course [31]. Through this system, universities can give students access to their courses, exams, and digital badges. This research addresses the limitations and the weakness of traditional e-learning platforms by proposing a micro-credentialing system that is built on blockchain technology to provide secure examinations and trustworthy and immutable digital badges for the students that represent all their achievements [31].

Terzi et al. [88] developed a digital system supported by blockchain for life-long learning. The BlockAdemiC project uses blockchain technology to build a secure, decentralized system for storing and verifying micro-credentials, educational tasks, certificates, diplomas, skills, and qualifications attained in higher education. To address the issues of certificate fraud that have not yet been dealt with satisfactorily, the lack of a formal representation, and the acknowledgment of informal and life-long learning outcomes, open-source blockchain technology is used to prevent certificate fraud in higher education and life-long learning domains and guarantees the confidentiality, privacy, integrity, and immutability of the information pertaining to degrees, certifications, and skills that students have achieved [88]. As a result, a safe, trustworthy, and transparent environment is built where stakeholders can verify their qualifications, certificates, skills, and micro-credentials. This system provides a solution that enables the creation of a digital education passport by offering a cryptographically secure wallet for safely managing all digital credentials pertaining to a student's education and training [88].

Ghonim and Corpuz [41] developed a new e-system for competency-based education (CBE) that uses blockchain technology. The digital CBE system evaluates practical activities as a result of a distinctive learning experience to highlight the strong and weak aspects of the required skills and competencies. The main objective of this research is the digitalization of competency-based education and the use of student e-portfolios as a suggested system for applied learning because the learning experience must align with industry expectations and new micro-credentials must be offered to indicate the acquired skills and competencies. By developing competency-based micro-credentials, the proposed digital CBE will strengthen the links between applied education institutions and businesses [41]. This system also accurately assesses learning experience outcomes and suggests the competency-based micro-credentials to be offered to employ-

ers. Moreover, it issues the micro-credentials that users can obtain by demonstrating their skills and competencies through the use of an electronic portfolio of evidence which is the result of learning activities. The use of blockchain technology as a solution in the digital CBE system makes it possible to securely store, issue, verify, and trace skills and competencies, improve the learning experience outcomes of the competency-based education approach in applied higher education institutions, and enhance the efficiency of CBE, curricula, and assessment techniques used in applied education. The difference between non-digital CBE and digital CBE revolves around the additional levels of the qualification framework's mapping and the use of blockchain technology [41].

Kumaresh [60] proposed an academic blockchain application in the education field to store students' certificates, achievements, credentials, and information on their additional skills/qualifications in the blockchain. The main objective of this study is to devise a method to store the data on students' records in the blockchain so stakeholders can access and validate student credentials easily. The use of academic blockchain makes it simple for stakeholders to track and identify fraudulent transactions in the education system as well as fake educational credits [60]. While digital badges make it easier to recognize a particular skill obtained by the student, one or more badges can be combined into an open badge passport in the academic blockchain and distributed throughout the network.
A consortium blockchain is more appropriate for academic blockchain. In this study, the authors used solidity to implement the academic blockchain and they ran a pilot study with only a small number of nodes participating, and the outcomes are evaluated in terms of transaction latency. The authors detected that a 100% threshold is required for a latency of 15 s [60]. The proposed application stores the student's credentials, grades, and achievements in a highly secure manner and has advantages in terms of cost and time. Additionally, it makes all these data available to stakeholders and employers to facilitate the recruitment process across the world and it makes the interaction between educational stakeholders easy and efficient [60].

Srivastava et al. [86] proposed a global trust credit transfer platform using blockchain technology in the education system to provide simple access to student credit transfers between universities and credit viewing by possible stakeholders. This system helps to validate the academic credentials of a student enrolled in a university that can be transmitted digitally among the stakeholders, such as higher education institutions and

companies. Additionally, it stores students' records, transcripts, and micro-credentials, as well as has an electronic credit transfer mechanism [86]. This credit system is based on tokens which are credit values that are granted to university students upon the successful completion of courses. This proposed platform is similar to the EduCTX platform [89] in that it creates a global decentralized credit transfer platform in higher education institutions. However, the EduCTX platform does not deal with the issue of a student enrolling in many courses under the same teacher, and the student is assigned a 2-2 multi-signature address [89]. On the other hand, their proposed platform offers a one-to-one multi-signature address between a student and a teacher for numerous courses. Both platforms are built based on an open-source Ark blockchain platform, a private and permissioned blockchain to ensure students' records are anonymized [86].

Alam et al. [15] discussed blockchain applications in the education field and their challenges. The authors also offered details about security, privacy, and trust in blockchain and proposed a digital credential framework based on blockchain. This proposed system will keep the student's information secure and allow students to verify their degrees for an indefinite period of time. This system also can make the verification process for micro-credentials, transcripts, and certifications easier and more reliable [15]. Students will obtain digital micro-credentials and an academic degree once they have completed all units of their academic program and have met the requirements for the degree. The students can also share their academic credentials with other stakeholders, such as employers and higher education institutions, by sending a specific identity to verify them. The main objective of this proposed system is to benefit from blockchain in several ways, such as storing, verifying, and sharing students' credentials quickly and easily in a secure manner [15].

2.4 Discussion of the Shortcomings of the Existing Literature Reviews

From the analysis of the selected research studies, several important findings on the issues that this thesis must address emerged in managing the micro-credentials field. This section categorizes these findings into four research gaps relevant to the management of micro-credentials for higher education students. In the following subsections, the four shortcomings of the previously selected studies are discussed. Detailed explanations of these research gaps can be found in Section 3.3 in Chapter 3.

Research Paper	Is the platform intelligent and trustworthy?	Does it use privacy-preserving techniques?	Does it provide specialization recommendations?	Does it use a multi-criteria decision mechanism?
Arenas and Fernandez [20]	No	No	No	No
Choi et al. [30]	No	No	No	No
Kishore et al. [58]	No	No	No	No
Lim et al. [63]	No	No	No	No
Turkanovic et al. [89]	No	No	No	No
Chukowry et al. [31]	No	No	No	No
Mikroyannidis et al. [71]	Yes	No	No	No
Mikroyannidis et al. [70]	Yes	No	No	No
Mikroyannidis et al. [69]	Yes	No	No	No
Mainetti et al. [65]	Yes	No	No	No
Terzi et al. [88]	No	No	No	No
Ghonim and Corpuz [41]	No	No	No	No
Kumaresh [60]	No	No	No	No
Srivastava et al. [86]	No	No	No	No
Alam et al. [15]	No	No	No	No

Table 2.4: Comparative analysis of the selected papers

2.4.1 Ability to manage micro-credentials based on an intelligent and trustworthy platform

Scant scholarly research has been conducted on micro-credentials in higher education to date. Public and private universities around the world, including Australia, are becoming increasingly interested in micro-credentials, which are the most recent innovation in online education after the COVID-19 pandemic [12]. Our analysis uncovered 15 existing articles that provide higher education micro-credential platforms using blockchain technology, as shown in Figure 2.1. These platforms address the issue of storing, validating, and accessing digital credentials in a secure manner, so they are easily available and widely accepted. The researchers use blockchain technology to provide direct manage-

ment and control over the micro-credentials that a student has acquired while ensuring ongoing protection and storage for them. The existing platforms for both categories PMM and IPMM are trustworthy platforms due to their use of blockchain technology.

As the existing IPMM platforms use AI techniques to provide personalized recommendations for the students as to what courses they should study next or which job position or learning pathway is appropriate, we consider these to be intelligent platforms [65], [69], [70], [71]. In this case, we view the platforms for the IPMM category as trustworthy and intelligent platforms. In contrast, the PMM platforms are considered to be trustworthy but not intelligent because they don't utilize AI techniques.

Although some of the existing studies have proposed blockchain-based micro-credential platforms with AI techniques, their intended uses differ from ours in the following ways:

1. Mainetti et al. [65] used blockchain technology and open badges to enable education credit transfer, while we used the same technologies to address the challenges related to micro-credential provenance.

   Furthermore, they did not address the privacy issue on a blockchain network regarding the exchange of student data between the stakeholders through their system. In addition, their proposed recommendation system is designed to provide students with advice on study materials and learning paths, so it does not make recommendations in relation to academic majors or action plans.

2. Mikroyannidis et al. [69, 70, 71] provided personalized course recommendations and job recommendations to help learners select their next course and their most suitable job based on their academic credentials and skills. However, they did not provide learning recommendations about academic majors to assist learners in selecting their future study areas. Moreover, the authors have not provided any proof to show the existence of the recommendation system to the readers, nor have they evaluated it or calculated its accuracy. In addition, they did not address the issue of privacy when sharing students' data with HEIs.

2.4.2 Ability to verify and share micro-credentials in a privacy-preserving manner

The existing micro-credential platforms make use of blockchain advantages as a decentralized architecture that provides security, confidentiality, durability, lucidity, and immutability [31]. Most blockchain platforms lack the ability to manage private data

because data on the ledger can be read by any node on the blockchain network [24]. Therefore, there is a need to provide an anonymous searchable service for student data. A blockchain-based micro-credential platform must implement anonymization techniques in order to preserve a student's real identity and ensure the privacy of student data on the blockchain [24].

The literature search undertaken in this thesis revealed that none of the existing studies address how students' data is shared in a privacy-preserving manner. Turkanovic et al. [89] and Srivastava et al. [86] are two studies that addressed the anonymous storage of student data on the blockchain. However, their main focus is not ensuring the anonymity of students' identities while securely exchanging data.

2.4.3 Ability to provide a proper recommendation for students' majors

The accreditation systems of the IPMM category provide personalized learning recommendations that will help students reach their academic and professional goals. Mainetti et al. [65], Mikroyannidis et al. [69, 70, 71] developed intelligent platforms that offer personalized recommendations to assist lifelong learners in reaching their personal and career learning objectives. These platforms of the IPMM category provide recommendations for course materials, learning paths, jobs that match the students' skills based on their educational credentials, courses that enable the student to obtain certifications, and the additional skills needed for the recommended job. However, none of these existing platforms offer learning recommendations for student's majors based on their micro-credentials.

Chukowry et al. [31], the micro-credential platform of the PMM category allows students to select their desired course, take the exam, and receive credit. Unfortunately, it cannot assist students in the course selection process by recommending the most suitable course to enable them to meet their educational goals. To summarize, none of the PMM and IPMM credential platforms provide recommendations for academic majors based on micro-credentials.

2.4.4 Ability to view all provided action plans and help students select a suitable one based on multiple criteria

To assist students in their decision-making, the system must be capable of predicting an appropriate choice based on a variety of factors. Students usually want to have access

to all action plans provided by multiple HEIs on a micro-credential platform in a single place. In order to help students select the most optimal action plan, the platform can filter them according to the student's preferred criteria, such as the location of the university, language, course duration, university rank, etc.

Unfortunately, none of the existing micro-credential platforms in both IPMM and PMM categories provide an approach to provide all the action plans in one place, nor an intelligent technique to filter many action plans and recommend an appropriate one according to the students' specific criteria.

Table 2.4 presents a comparative analysis of the 15 selected studies against specific criteria, aimed at determining whether each study addresses any of these issues. This thesis aims to address all the above shortcomings by proposing an intelligent decision support system to help in the management of micro-credentials for students in the higher education sector. The proposed framework will be a trusted and intelligent blockchain platform for managing micro-credentials (detailed in Chapter 5).

2.5 Conclusion

This chapter provided a thorough review of the relevant literature to help readers understand the current state of the work on blockchain-based micro-credential platforms in HEIs. Moreover, it identified the research needs surrounding the management of micro-credentials based on blockchain technology in the higher education sector. The SLR approach was used to review the various approaches that have been proposed for the existing blockchain-based micro-credential platforms. This review helped identify their style of working and find the research gaps and research objectives. Based on our analysis, we found only 15 studies that offer blockchain-based micro-credential platforms in HEIs. These articles have been critically analyzed for further clarification, and compared against the four shortcomings.

The next chapter presents the research gaps found as a result of the literature review reported in this chapter. The research questions and objectives are also presented in the following chapter.

CHAPTER 3

RESEARCH QUESTIONS AND OBJECTIVES

3.1 Introduction

In Chapter 2, we presented a systematic review of the existing literature and we identified four shortcomings that need to be addressed in this thesis. We noted that several researchers have achieved significant advances in the field of managing micro-credentials. However, none of the existing systems present a completely intelligent solution for managing micro-credentials for both students and higher education institutions (HEIs). This chapter formulates the research objectives by identifying the research questions based on the comprehensive SLR presented in the previous chapter.

The research questions serve as a guide for formulating the objectives which are presented in this chapter. This chapter is organized as follows: 3.2 presents a set of definitions for the terminologies that are used in this thesis. Section 3.3 outlines the research gaps that provide the motivation for conducting this thesis. Section 3.4 details the main research question and the sub-questions. Section 3.5 presents the research objectives of this study. Section 3.6 concludes this chapter.

3.2 Keywords Definitions

This section defines the research terminologies which are used in this thesis.

3.2.1 Blockchain

Blockchain is a chain of blocks, where each block is cryptographically connected to the preceding block and time-stamped [93]. A block is a collection of data that contains a list of signed transactions and the hash of the previous block. The chain is immutable and secure, and every new block is appended to the end to increase the length of the chain. Transactions can be recorded in a shared ledger within a community of users, and they are exchanged by peers of the blockchain network [92].

3.2.2 Hyperledger fabric

Hyperledger Fabric is an open-source blockchain platform from the Linux Foundation [13]. It was created to offer the required frameworks, standards, tools, guidelines, and libraries to build blockchain-based software and associated applications for use across different industries. It is a blockchain technology that allows organizations to build and use their own private or permissioned blockchain networks [42].

3.2.3 Chaincode

Chaincode also known as smart contracts, is software that can be used to read and run data on the blockchain ledger [5]. It is an executable code that is invoked on the blockchain to perform an agreement between parties. Smart contracts record all transactions that have occurred in the network [79].

3.2.4 Micro-credential

Micro-credential is evidence of the learning achievement that verifies a learner's knowledge, skills, and experience which has been acquired following a short learning experience in a given subject area or capability [47]. It is a type of learning certificate that can be aggregated into a larger credential or degree to demonstrate an individual's level of learning. It is also known as a micro-degree, nano-degree, digital badge or digital credential [36].

3.2.5 Academic degree

Academic Degree is a qualification conferred on students by a college or university when they have completed a course of study at a particular level, for example, a bachelor's degree, a master's degree, or a doctorate [53].

3.2.6 Academic major or specialization

Major is a subject or course in a particular area in which students specialize during their university candidature to acquire an academic degree in this specific subject [72].

3.2.7 Action plan or learning plan

Action Plan is a learning plan completed by a learner to achieve a specific goal [48]. This plan includes a list of actions that must be performed well to reach the required academic degree and to identify how their newly acquired abilities or skills will be applied. The learning action plan plays a crucial role in ensuring a learner's knowledge is maintained and practiced after their study has been completed [27].

3.2.8 Higher education institution (HEI)

Higher Education Institution is any private or public post-secondary institution that operates in the higher education (HE) section to award academic degrees or certificates [33] to students upon completion of a course. HEIs include universities, colleges, and professional-oriented institutions [52].

3.2.9 Multi-criteria decision making (MCDM)

MCDM is a process for evaluating options to assist in complex decision-making. It helps to determine the best alternative to solve a complex problem by considering multiple criteria to achieve a specific goal [11].

3.2.10 Privacy-preserving techniques (PPTs)

PPTs are powerful cybersecurity techniques that protect data by providing security when it is transferred between several parties, so a third party does not know what data is shared between the parties [59].

3.2.11 Recommender system (RS)

Recommender system or recommendation system is an information management system that generates recommendations to users for items or products based on their preferences and helps them to conveniently access information online [74].

3.2.12 Intelligent Blockchain for Managing Micro-credentials (IBMM)

We use the term *Intelligent Blockchain for Managing Micro-credentials (IBMM)* is the platform proposed in this thesis to provide services to students and higher education providers related to micro-credentials and to achieve the main goal of this research.

3.2.13 Privacy-aware sharing process

We define: *Privacy-aware sharing process* as a process that helps to protect the data and provides privacy for personal information by isolating it when sharing data across educational institutions. It also provides tools for privacy-awareness support so informed decisions can be made about the disclosure of data.

3.2.14 Intelligent action plan selection

We define *Intelligent action plan selection* as a process that addresses the issue of selecting the right action plan provided by many different educational institutions for students who need access to the best action plan that aligns with their preferences.

3.3 Research Gaps

This section outlines the research gaps that were identified from the existing literature which will be addressed in this thesis. Please see Section 2.4 in Chapter 2 for further details.

3.3.1 Research Gap 1: Few of the existing studies provide an intelligent and trustworthy platform for managing micro-credentials in HEIs.

The main objective of this research is to develop a trusted and intelligent blockchain-based micro-credential platform for higher education students. This would be a significant initiative for advancing technology in higher education, enabling large numbers of learners and multiple domestic and foreign HEIs to join a secure platform. Additionally, the developed platform would allow learners to shape their lifelong learning pathways and share their micro-credentials with other stakeholders in a secure and verified

manner.
Our literature search revealed only a limited number of sources offering intelligent and trustworthy micro-credential platforms based on blockchain technology. The platforms of the IPMM category are trusted and intelligent micro-credential platforms since they rely on artificial intelligence (AI) techniques and blockchain technology. They use the blockchain for verifying and storing micro-credentials in a secure environment, the AI techniques are used for offering personalized recommendations. However, there are differences between these existing platforms and our developed platform as described in Section 2.4 in Chapter 2.

3.3.2 Research Gap 2: None of the existing studies use a privacy-preserving technique to verify and share micro-credentials in a privacy-preserving manner.

This research addresses the issue of privacy for students by anonymizing their real identities when sharing their educational credentials with other HEIs. To ensure the security and privacy of student information, we need to anonymize students' identities such as names, email addresses, etc., on the blockchain to safeguard the privacy of the student's data in the micro-credential platform.
None of the existing studies have specifically focused on the anonymization of students' data through credentials exchange, even though they have addressed the issue of anonymous storage of student data on the blockchain.

3.3.3 Research Gap 3: None of the existing studies provide a recommender system to predict the appropriate major for a student to complete a certain degree based on micro-credentials.

While some existing studies provide personalized learning recommendations about jobs or courses, none have developed a recommender system that can assist students in selecting a major based on their acquired micro-credentials. This research addresses the issue of learning recommendations for higher education students who require assistance in choosing a suitable specialization. We propose an intelligent technique to provide support for new university students by offering recommendations about majors that match their micro-credentials to help them complete their academic degrees.

3.3.4 Research Gap 4: None of the existing studies provide a system to help students display all the offered action plans from many HEIs in a single view, nor is there an intelligent mechanism to assist a student in selecting the most suitable action plan based on certain preferred criteria.

There are no existing studies that provide a mechanism for displaying all the students' action plans from multiple HEIs in one place and enabling students to select the most appropriate one using an intelligent technique that takes into account multiple criteria. This study examines how students can find multiple action plans provided by several HEIs on a single platform and predict the most appropriate one based on their specific criteria. We provide a mechanism that allows students to access all action plans offered by several HEIs in a single interface. Moreover, we utilize an intelligent technique to assist students in choosing the most appropriate action plan based on their preferences. This solution will provide a more efficient approach for students in selecting their action plans.

3.4 Research Questions

This section presents the main research question and the sub-questions that we answer to intelligently solve the problem of managing micro-credentials in HEIs. The main research question is as follows:

How can micro-credentials be verified, shared, and intelligently analyzed to help a user select a future academic major and action plan?

We divide the main question into five sub-questions, which are presented below. These sub-questions provide a more detailed understanding of the research topic and are addressed in the subsequent chapters of the thesis.

- **RQ1:** How do we develop an intelligent and trustworthy platform for managing and maintaining micro-credentials?
- **RQ2:** How can micro-credentials be shared taking into account the student's privacy?

- **RQ3:** How can a recommendation for a major be generated so that the students can complete their degree?

- **RQ4:** How can action plans from various educational institutions be collected to help students complete their desired degree and how can they be assisted in selecting an action plan based on certain preferred parameters?

- **RQ5:** How can the proposed solutions be evaluated using a proof-concept framework?

3.5 Research Objectives

This section presents a high-level overview of the five research objectives that drive the main objective of this thesis which is to develop and evaluate a reliable and intelligent blockchain-based micro-credential platform. The platform will be designed with five specific objectives in mind as follows:

1. Develop an intelligent and trustworthy platform for managing, sharing, and storing micro-credentials on the blockchain.

   To address this objective, we use blockchain technology to develop a micro-credential platform called Intelligent Blockchain for Managing Micro-Credentials (IBMM). This platform will store, manage, share, and verify students' micro-credentials on the blockchain network. This objective addresses the first research question (RQ1) and Chapters 4 and 5 provide a detailed explanation.

2. Apply a privacy-preserving technique for sharing micro-credentials with HEIs which considers the students' privacy on the blockchain.

   To address this objective, we apply a privacy-preserving technique (PPT) to provide privacy for students on the blockchain, so micro-credentials can be shared and verified securely while preserving the students' identities on the blockchain. This technique helps to anonymize a student's real identity on the blockchain when they share their micro-credentials with HEIs. This objective addresses the second research question (RQ2) and Chapters 4 and 5 provide a detailed explanation.

3. Apply an intelligent technique to generate learning recommendations for students about academic majors to complete a specific degree.

   To address this objective, we develop a recommender system by applying an intelligent technique and choosing machine learning algorithms that can correctly predict a suitable major for a student based on their micro-credentials. This solution will help students to know which major is compatible with their previous micro-credentials and academic qualifications to attain a particular academic degree. This objective addresses the third research question (RQ3) and Chapters 4 and 6 provide a detailed explanation.

4. Assist students in collecting and viewing all action plans provided by several HEIs in one place. Furthermore, to apply an intelligent mechanism to help students select the most appropriate action plan based on their preferred parameters.

   To address this objective, we collect all action plans for a student that have been offered by multiple HEIs and store them on the blockchain to assist students in easily accessing them from one place. We achieve this objective by allowing every HEI to upload and store the details of the generated action plan on the blockchain and associate it with a student's profile. Then, we apply intelligent algorithms to predict the most suitable action plan for a student to help them choose one of the multiple action plans according to their selected criteria. This objective addresses the fourth research question (RQ4) and Chapters 4 and 7 provide a detailed explanation.

5. Build a prototype system to validate and evaluate the effectiveness of the proposed methodology from objective 1 to objective 4.

   To address this objective, we evaluate the proposed IBMM platform by using the Hyperledger Fabric blockchain and apply the privacy-preserving method to achieve objective 2. Moreover, we use machine learning and AI techniques to evaluate the results of objectives 3 and 4. This objective will be achieved by verifying each proposed solution for all the objectives to assess their effectiveness. This objective addresses the fifth research question (RQ5) and Chapters 4, 5, 6, and 7 provide a detailed explanation.

3.6 Conclusion

This chapter clarified the meaning of some of the research terminologies that we use in this thesis. It also outlined the main research gaps that need to be addressed to solve the main research problem in this thesis. Moreover, this chapter introduced the research questions and research objectives that were elicited from the limitations in the existing literature.

The next chapter presents the research methodology used to design and develop the proposed solution and provides an overview of the proposed solution to the research problem. In addition, an overview of the proposed solution for each of the four research questions that need to be addressed in this thesis is presented. The detailed framework of the Intelligent Blockchain for Managing Micro-credentials (IBMM) platform is also described in the next chapter.

CHAPTER 4

IBMM: SOLUTION OVERVIEW

4.1 Introduction

As discussed in Chapter 2, even though many studies in the existing literature examined the issue of how to manage, verify, and store micro-credentials, there are still open and unsolved research issues. In this thesis, four research gaps are identified and addressed. The research gaps, questions, and objectives were defined in Chapter 3. This chapter presents the research methodology used in this thesis and an overview of the proposed solutions for each of the identified research questions.

This chapter is structured as follows: Section 4.2 presents an overview of the research methodology used to address the main research question. Section 4.3 provides an overview of the proposed solutions to research questions (RQ1-RQ5). Section 4.4 concludes this chapter.

4.2 Selected Research Methodology

This thesis tackles the stated problem by creating, testing, and evaluating a methodology. To address the four research gaps detailed in Chapter 3, we follow a scientific methodology that will help establish the validity and reliability of the proposed solutions. This section gives an overview of the design science research methodology (DSRM) which is selected

as the research methodology for the research problem. An overview of the DSRM process model is presented in Figure 4.1, showing the main steps that are followed to address the identified gaps [56]. DSRM is divided into the following six phases [56]:

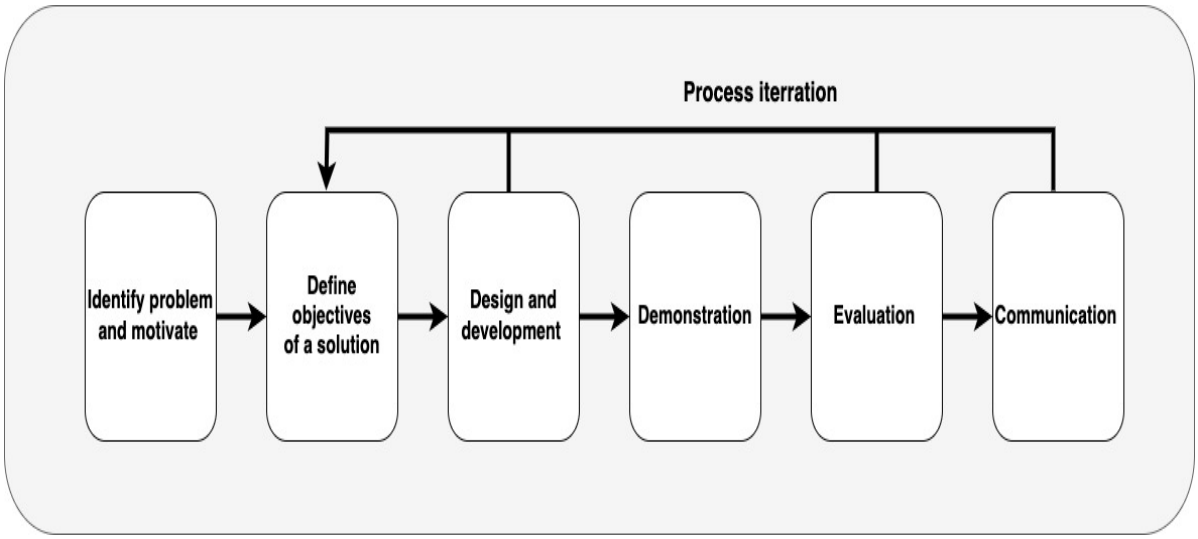

Figure 4.1: DSRM process model

1. Problem identification and motivation phase.
   In this phase, the existing studies on topics related to micro-credential management in the higher education sector are retrieved and reviewed to identify the problem and motivation. Based on the identified problem, we outline the research gaps that need to be addressed by analyzing the existing literature using a systematic literature review (SLR). This process is documented in Chapter 2.

2. Define the objectives and a solution phase.
   After the research gaps are identified in step one, we set the research objectives and devise a conceptual solution to the problem. The focus of this study is to develop an intelligent blockchain-based micro-credential framework to manage, share, and store students' micro-credentials and apply intelligent methods to recommend majors and select the best action plan for students. This phase is documented in Chapters 3 and 4 of this thesis.

3. Design and development phase.
   In this phase, we design a blockchain framework and a privacy-preserving technique for the solutions to research questions RQ1 and RQ2. Subsequently, we develop prototype systems using artificial intelligence (AI) and machine learning

(ML) models for the solutions to research questions RQ3 and RQ4 which are used to validate and test the selected models as a part of the overall methodology. This phase is documented in Chapters 5, 6 and 7.

4. Demonstration phase.
   To demonstrate the efficiency of the proposed IBMM framework in solving the identified problem, we develop a prototype system to address research questions (RQ1-RQ4). We also demonstrate the effectiveness of the techniques used to address the research gaps. An effective understanding of how to use the method to address the problem is necessary for the demonstration. This phase is documented in Chapters 5, 6 and 7.

5. Evaluation phase.
   In this phase, we assess and validate our proposed methodology using the results from the previous phase. We use a number of well-known metrics to evaluate the performance of the ML and AI models. Subsequently, we can choose whether to return to the design and development phase to improve the method's effectiveness or go to the evaluation phase and leave further improvement to future initiatives. At the end of this phase, we optimize our proposed methodology based on the results of the evaluation and validation. This phase is documented in Chapters 5, 6, and 7.

6. Communication.
   In this phase, scholarly research publications are submitted to international peer-reviewed journals and conferences relating to the blockchain-based micro-credential area. The researchers write papers about the outcomes from the previous phases. This phase is undertaken on a regular basis.

During the research process, the design and development phase and the evaluation phase are performed iteratively based on the results obtained. In order to facilitate a deductive cognitive process, namely, the development and evaluation of the solution as the research is being completed, this iteration represents a progression from partially completing the research to defining clear research objectives.

4.3 Solution Overview

This section overviews the proposed solution for the IBMM framework that is developed to intelligently manage, verify, and store micro-credentials for higher education students. To address the five research questions outlined in Chapter 3, we apply several techniques such as privacy-preserving techniques, AI, and ML methods. The following subsections provide overviews of the proposed solutions for research questions (RQ1-RQ5).

4.3.1 Solution overview for research question 1: General architecture of the IBMM

The main objective of this research is to design and develop an intelligent blockchain platform for managing micro-credentials in higher education institutions (HEIs). This section presents an overview of the ***Intelligent Blockchain for Managing Micro-credentials (IBMM)*** platform which is developed to store, manage and verify students' micro-credentials on the blockchain network. The detailed solution for the research question RQ1 is presented in Chapter 5. Hyperledger Fabric blockchain was chosen to design the IBMM framework from end to end due to the numerous benefits it offers, including the following key characteristics [13]:

- Open-Source: it is an open-source blockchain framework managed by the Linux Foundation, designed to create distributed ledger applications or solutions. A large and active team of developers and collaborators ensures that the software is continuously improved, bug-fixed, and kept secure [13].

- Security: it is a private (permissioned) blockchain network that provides strong control over network participation and limited access, ensuring high levels of security, confidentiality, flexibility, robustness, and scalability. It offers a high level of security for sensitive data to ensure it is stored and transmitted securely [13].

- Scalability: it uses a unique consensus technique that allows two parties to agree on a transaction without any third-party interference or observation. This consensus technique is called Practical Byzantine Fault Tolerance (PBFT), which enables high performance while ensuring scalability and consistency on the blockchain network. Scalability is a crucial feature when dealing with a large number of transactions per second [13].

- Smart Contracts: it uses smart contracts known as chaincode which are self-executing applications for automating business principles [13].

A common design pattern for a distributed system development is the model-view-controller (MVC) architecture [37]. Based on this architecture, the IBMM platform consists of three layers, namely the view layer, the controller layer, and the model layer as shown in Figure 4.2 [17].

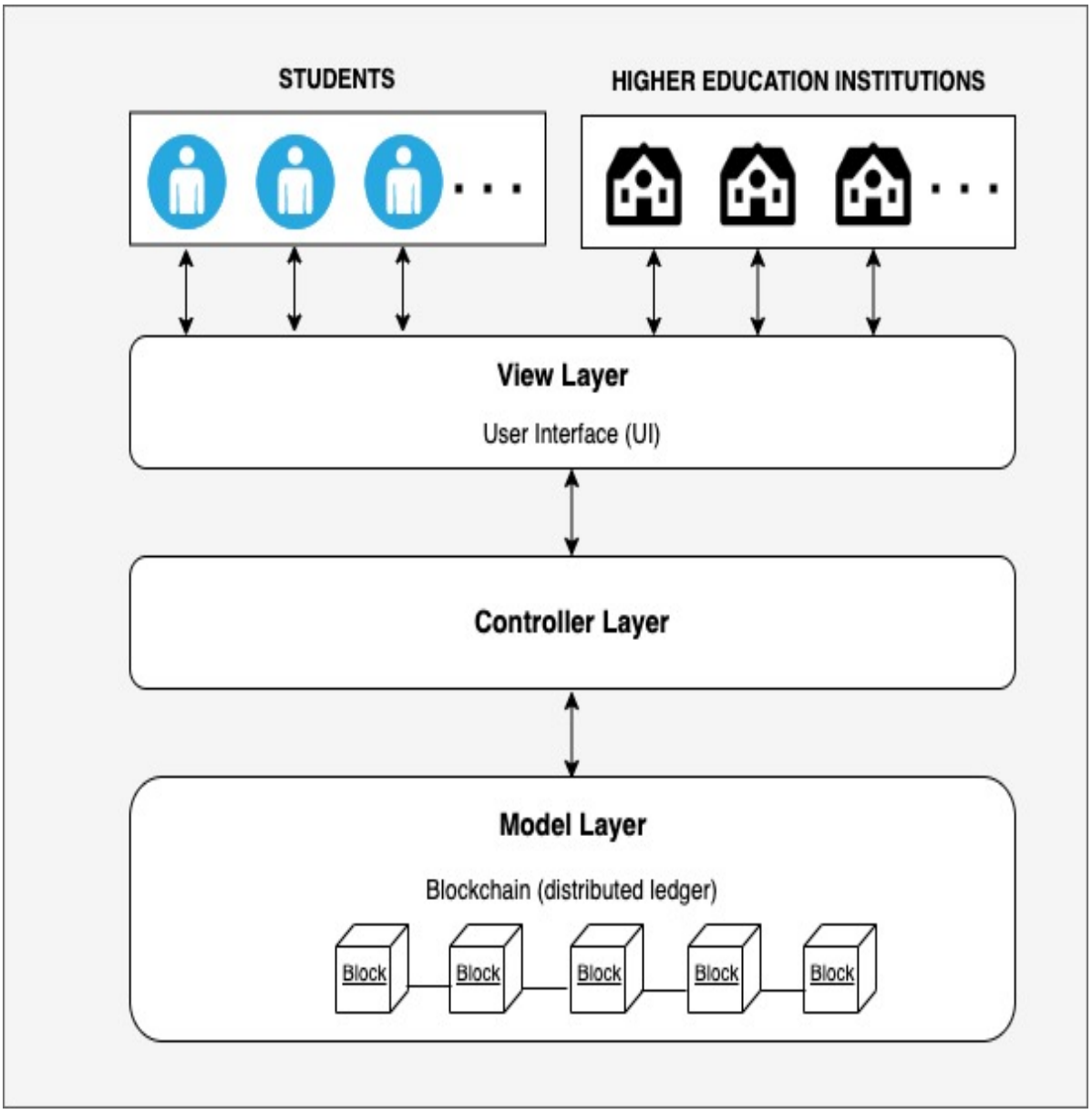

Figure 4.2: General architecture of the IBMM Platform (Alsobhi et al. [17])

1. **The view layer:** This layer is the user interface (UI) which shows the outputs to a user. Internal and external users i.e., students and HEIs can interact with the IBMM framework via this layer. Through this layer, students can send requests, and view the results and their profiles. This layer also allows HEIs to view students' profiles and send micro-credentials and action plans to the blockchain ledger [17]. In addition, both students and HEIs can register with the IBMM platform via this layer.

2. **The controller layer:** This layer is the link between the view and model layers. It receives input from the user and converts it to queries for the model layer and it also controls how the data is displayed. This layer also conducts customized activities and executes them using artificially intelligent algorithms in the form of smart contracts, such as personalized recommendations to students, etc. [17].

3. **The model layer:** This layer is the blockchain layer which is a distributed ledger to verify all the completed data transactions, including micro-credentials, and store them on blocks in a secure, trusted, and private ledger. This layer contains the data logic written in smart contracts to simply verify and store micro-credentials on the blockchain layer [17].

4.3.2 Solution overview for research question 2: Preserving student's identity privacy during data sharing

This section provides a brief overview of the proposed solution to research question two (RQ2), and in Chapter 5 a more comprehensive description is given. To address this research question, we apply a privacy-preserving technique within the blockchain platform. This technique ensures the secure sharing of micro-credentials on the blockchain while protecting the students' identity [23]. Thus, student micro-credentials can be securely shared with other HEIs using cryptographic hashing. We develop a privacy-aware sharing process that uses a one-way hash function. The one-way hash method was chosen because retrieving the input data from the hash value is computationally impossible. Unlike encryption, hashing prevents recipients from reverse-engineering the process of decrypting messages [78]. Using the one-way method ensures that unauthorized parties cannot obtain the original data even if the hashed data is compromised. Moreover, it is an effective method for providing security and privacy while protecting sensitive information and allowing students to remain anonymous while participating in data

sharing [78].
We employ the one-way hash algorithm (SHA-256) to convert a real student's identity into a unique and irreversible hash value by developing smart contracts that control the process of anonymizing a student's identity within the IBMM platform. The hash value can be used as a unique identifier or a pseudo-identity for students to maintain their privacy while HEIs can access and verify the students' micro-credentials without revealing their identities. The benefit of the privacy-aware sharing process is to facilitate efficient collaboration and micro-credential exchange between several HEIs, enabling a safer and more efficient educational ecosystem. Figure 4.3 illustrates the process of hashing a student's identity and generating a pseudonym. The following steps describe the process of how to generate a unique pseudonym for a student:

1. During registration, the student sends their personal information, such as name, date of birth, email address, etc. through the view layer to store this data on the blockchain.

2. The blockchain receives the data and invokes the smart contract that is responsible for generating pseudonyms.

3. The hashing algorithm is applied separately to the student's name and email address, and two different hash values are generated.

4. These two hash values are combined, and then the hashing algorithm is applied again to the combined output to generate a unique identifier/pseudonym for the student.

5. The student can share this pseudonym with several HEIs off-chain, while the student's identity is anonymized to maintain data integrity and security. Both the real identity and pseudonym of the student are stored on the blockchain.

4.3.3 Solution overview for research question 3: Providing learning recommendations for students' majors

An overview of the proposed solution to research question three (RQ3) is presented in this section, and a more detailed description can be found in Chapter 6. Based on AI and ML techniques, we develop a recommender system that addresses this research question. The following steps are involved in developing a recommender system to recommend the most suitable academic major for a student:

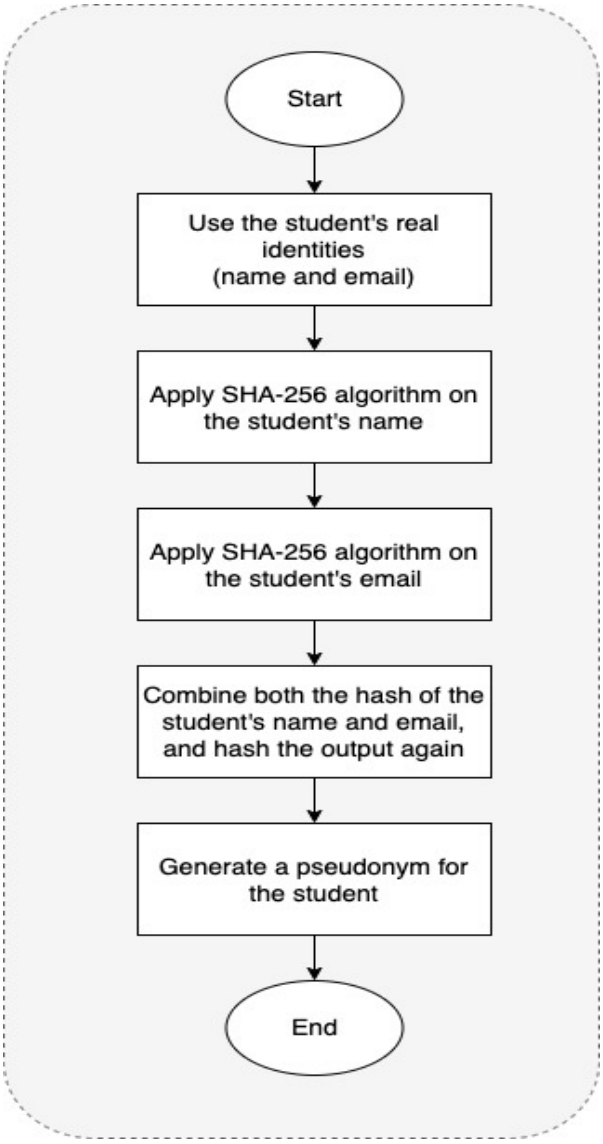

Figure 4.3: Workflow of hashing a student's identity and generating a pseudonym

1. Data collection: in this stage, real data is collected from students studying at universities in Australia and Saudi Arabia. An online survey is used as a method to collect the data. The survey explores and models the relationship between the previous and future education qualifications of students aspiring to pursue higher education. The survey consists of several questions for students about their educational background, previous qualifications, previous academic majors, micro-credentials, educational interests, personal data, and other relevant details that may be helpful in making recommendations. It is possible to build a model capable of accurately predicting the most appropriate academic major for a student

by uncovering relevant features. Further details of the dataset are presented in Chapter 6.

2. Data analysis and feature selection: upon completion of the data collection phase, we preprocess and analyze the dataset. We use this analysis to identify relevant features, patterns, and correlations, which can contribute to predicting an appropriate major for a student. The data analysis process provides insights into the dataset and helps us understand how the data is related. We split the dataset into two sets, one for training and one for testing.

3. Model development: ML and AI algorithms are used to predict suitable majors for students. The classification algorithms used are XGBoost, random forest, LightGBM, and multilayer perceptron (MLP). The selected models are learned and predictive models that are able to tie specific student attributes to certain academic majors are developed.

   The XGBoost, LightGBM, random forest, and MLP algorithms are selected as they are widely used for a variety of classification tasks. Additionally, they are highly efficient and robust execution methods [28, 84]. The XGBoost is a powerful machine-learning algorithm that assists in understanding data and making better decisions. There is no need for parameter optimization or tuning, and it can be used directly after installation without any additional configuration, which can increase the model's performance [84]. The random forest algorithm is stable against noise and can process numerical and categorical data easily without suffering from overfitting [28]. The LightGBM is a fast algorithm in training and achieves high performance [21, 57]. The MLP is capable of learning nonlinear models in real-time, as well as making quick predictions [7].

4. Evaluation and validation: the training and testing process ensure the accuracy of the models. We use several well-known evaluation metrics, such as accuracy, precision, recall, and F1-score to evaluate the model's performance.

   Once the aforementioned steps are completed, a recommender system is created to recommend suitable majors for students. The recommendation process is depicted in Figure 4.4.

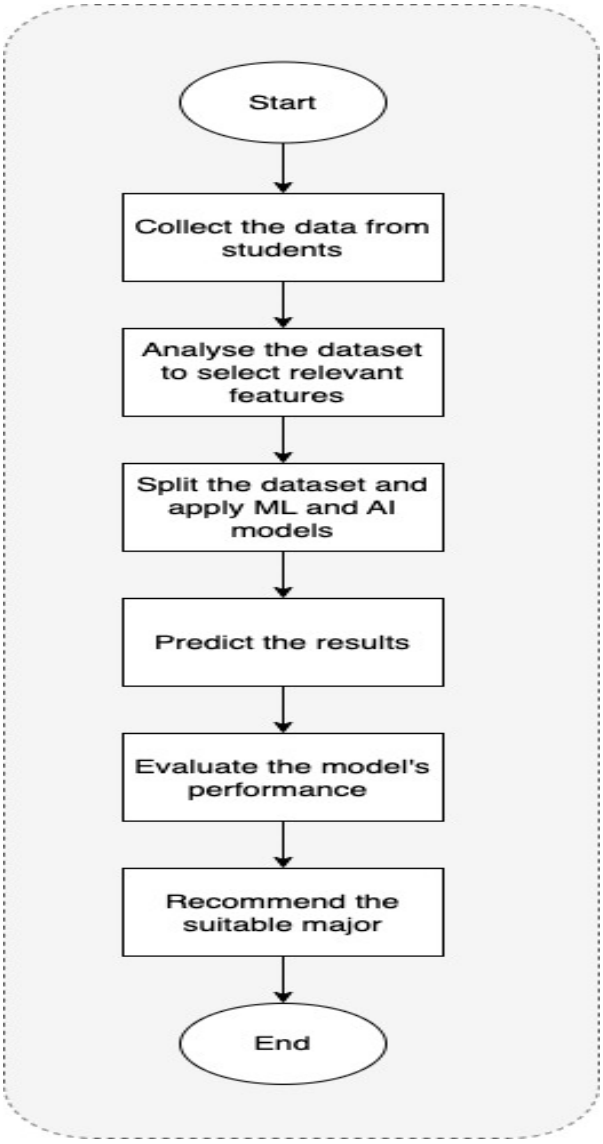

Figure 4.4: Workflow of the recommendation process

4.3.4 Solution overview for research question 4: Collecting and selecting action plans intelligently

This section provides an overview of the proposed solution to research question four (RQ4), while Chapter 7 offers a more detailed description. Students who request action plans from several HEIs must share their pseudonyms off-chain. Upon receipt of the pseudonym, the HEIs can use it to access the student's profile to verify their academic qualifications and micro-credentials. These data help HEIs create customized action plans that guide students to complete their degree programs. To address this research

question, we divide the proposed solution into two stages as follows:

1. Action plan collection: to collect the action plans, every HEI is required to upload action plans to the IBMM platform to ensure a unified and comprehensive view of all the generated action plans for students. This platform serves as the main repository for storing student data on the blockchain ledger and associating it with the student's profile.

2. Action plan selection: to choose the most optimal action plan among multiple options based on certain criteria, ML models are used. The ML algorithms used are XGBoost (Pairwise), XGBoost (NDCG), and LightGBM. The ML models are learned and predictive models which are able to connect specific student attributes to a certain action plan based on the selected criteria are developed. The training and testing process ensures the accuracy of the models.
   Both XGBoost and LightGBM models are efficient ML algorithms that are often used in ranking tasks. We chose them due to their many advantages, including high performance, speed and efficiency, scalability, faster training, high accuracy, preventing overfitting, and requiring less memory [21, 57, 84].

Upon completion of the action plan collection phase and before applying the ML models, the dataset is analyzed to provide comprehensive information on each student, including personal information, academic background, micro-credentials, selected criteria, and action plans. This analysis aims to evaluate the criteria selected by the student and define relevant features that can assist in the selection process. The dataset is divided into two sets, training and testing. Figure 4.5 illustrates the process of collecting all action plans in one place and selecting the most appropriate one.

4.3.5 Solution overview for research question 5: Evaluation of research questions 1,2,3, and 4:

- Evaluation of the proposed solution for RQ1: a detailed explanation of this is presented in Chapter 5. We develop a software prototype for the IBMM architecture which serves as a proof of concept, so no validation is necessary for the first research question. We use a Hyperledger Fabric blockchain platform to develop the software prototype. This is the most critical objective of this research as it provides a proof of concept to evaluate the system. In the following, we evaluate the proposed solutions for each of research questions 2,3 and 4.

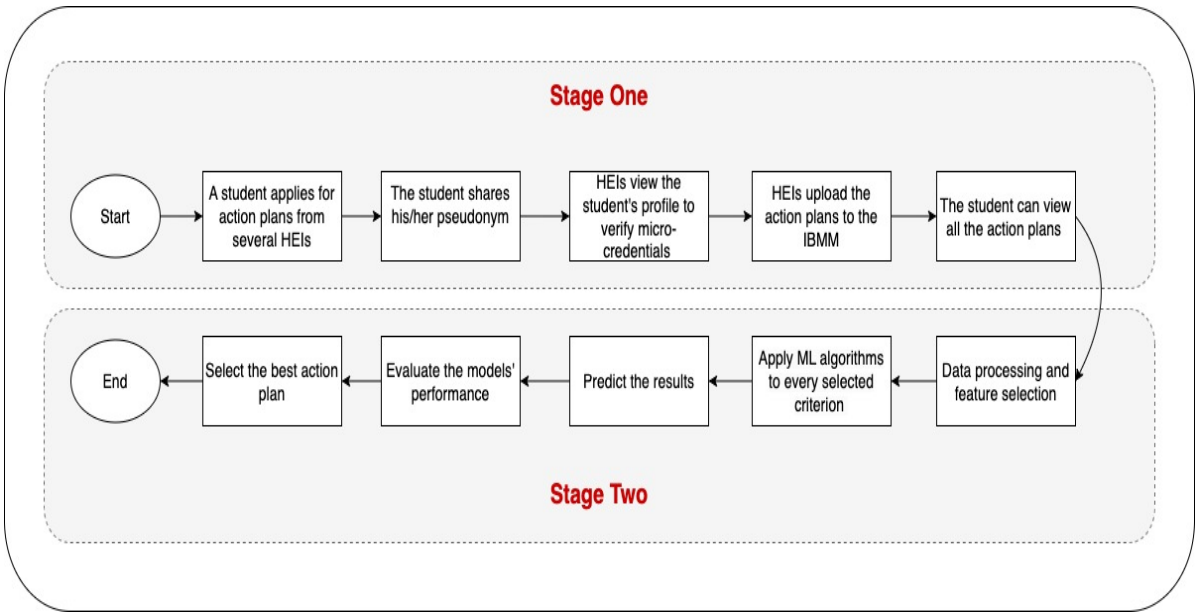

Figure 4.5: The process of collecting and selecting action plans

- Evaluation of the proposed solution for RQ2: a detailed explanation of this is presented in Chapter 5. The following steps provide an overview of the evaluation process for preserving student identity during data sharing.

  1. Select a sample of 100 students from the dataset that is collected to address research question RQ3, as described in Chapter 6.
  2. Generate a pseudonym for each student based on their identity (name and email address) by applying the one-way hash algorithm.
  3. Use each student's pseudonym to access and view their profiles.
  4. Evaluate the validity of the chosen algorithm by determining if the student's real identity has been revealed when viewing their profile.

- Evaluation of the proposed solution for RQ3: a detailed explanation of this is presented in Chapter 6. Following is an overview of the evaluation process of the developed recommender system that provides recommendations for students' majors:

  1. Conduct an online survey of university students to collect information about their personal and academic information and their previous and desired majors.

2. Apply the selected ML and AI algorithms (XGBoost, LightGBM, random forest, and MLP) separately to the dataset to intelligently recommend the most suitable major for each student using their features.
3. Evaluate each model's performance by calculating the accuracy using the following equation:
   Accuracy = (Number of correct recommendations)/ (Total number of recommendations) * 100
4. Compare the performance of all models and select the model with the highest accuracy.

- Evaluation of the proposed solution for RQ4: a detailed explanation of this is presented in Chapter 7. Following is an overview of the evaluation process of selecting the most optimal action plan for a student based on several criteria:

  1. Create a new dataset containing information about action plans/courses.
  2. Apply the selected ML algorithms (XGBoost (Pairwise), XGBoost (NDCG), and LightGBM) separately to the dataset to intelligently select the most optimal action plan for each student based on multiple criteria.
  3. Evaluate each model's performance by calculating the accuracy using the following equation:
     Accuracy = (Number of correct predictions based on the selected criteria)/ (Total number of predictions) * 100
  4. Compare the performance of all models and select the model with the highest accuracy.

Further explanation about the research methods used to address each research question can be found in the upcoming chapters as follows: Chapter 5 provides an in-depth explanation of the proposed solution designed to address both the first research question which is related to the IBMM framework's development and the second research question which involves the implementation of a privacy-preserving technique. In addition, Chapter 6 presents a comprehensive explanation of the proposed solution designed to address the third research question, which pertains to the recommender system's development. Lastly, Chapter 7 offers also a more detailed description of the proposed solution to the fourth research question, which revolves around the multi-criteria selection process.

4.4 Conclusion

This chapter presented the selected research methodology that was used to address the research gaps identified in Chapter 3. The general architecture of the IBMM framework was presented and the process involved in building this framework was also discussed. Finally, an overview of the proposed solutions to each of the five research questions RQ1-RQ5 in this thesis was provided.
The next chapter provides more detailed explanations of the proposed solutions to the first and second research questions regarding the IBMM platform's development and ensuring the privacy of students' identities on the blockchain.

CHAPTER 5

IBMM: Intelligent Blockchain for Managing the Micro-credential Framework and the Privacy-Preserving Technique

5.1 Introduction

Chapter 3 explained the research issues, objectives, and questions identified from the extensive systematic literature review reported in Chapter 2, followed by an overview of the proposed solutions for each research question outlined in Chapter 4. This chapter provides a comprehensive solution to the first and second research questions and discusses the proposed methodologies in further detail. The focus of this chapter is on presenting a blockchain-based solution that efficiently helps to manage, store, share, and verify micro-credentials intelligently for higher education students. This solution is particularly useful for students who are interested in pursuing higher education. Moreover, a privacy-preserving technique is proposed to securely share the micro-credentials of students while preserving their real identities.

This chapter is structured as follows: Section 5.2 introduces the general architecture of the IBMM framework as a blockchain-based higher education micro-credential platform and discusses the various components associated with this platform. Section 5.3 presents the development of the Hyperledger Fabric blockchain as the proposed solution for addressing the first research question. Blockchain is described in this section in

detail, as well as how it works within the IBMM system. A privacy-preserving technique employed to guarantee a student's data privacy when sharing micro-credentials with HEIs is presented in Section 5.4. That is the proposed solution to the second research question. Section 5.6 discusses a prototype evaluation in order to assess the performance and functionality of the designed solution. The developed prototype is described in this section to provide valuable insights into its practical aspects. Section 5.7 concludes this chapter.

5.2 General Architecture of the IBMM Framework

This section presents a comprehensive description of the architecture of the Intelligent Blockchain for Managing Micro-Credentials (IBMM), which serves as the proposed solution to address RQ1. The first research question is ***How do we develop an intelligent and trustworthy platform for managing and maintaining micro-credentials?***. We explain the platform's functionality and operation, its components, and working principles. Moreover, we describe in detail the architecture of the platform, emphasizing the use of blockchain technology to ensure security and reliability. The main purpose of this platform is to store, manage, and verify students' micro-credentials in a reliable and intelligent manner. Furthermore, the platform is able to verify and store micro-credentials, and personal and academic data on the blockchain. With this platform, students can securely share their academic profiles with several HEIs while ensuring the anonymity of their real identity. In addition, the IBMM uses intelligent techniques to offer personalized learning recommendations in order to assist students in choosing a suitable major and action plan to complete a specific degree. The IBMM platform performs the following main tasks [17]:

- Manage, verify, and store students' micro-credentials on the blockchain ledger.
- Allow multiple HEIs to access students' profiles and micro-credentials in a privacy-preserving manner.
- Allow students to access their micro-credentials and profiles from anywhere and at any time using a unified platform.
- Provide learning recommendations for students' majors based on their micro-credentials and academic achievements.

- Help students in selecting the most suitable action plan from several options based on multiple criteria to pursue their learning.

5.2.1 The design structure of the IBMM platform

The structure of the IBMM framework comprises three layers, namely ***the view layer, the controller layer, and the model layer*** as described in Chapter 4 in Section 4.3.1. The design structure of the IBMM platform is presented in Figure 5.1.

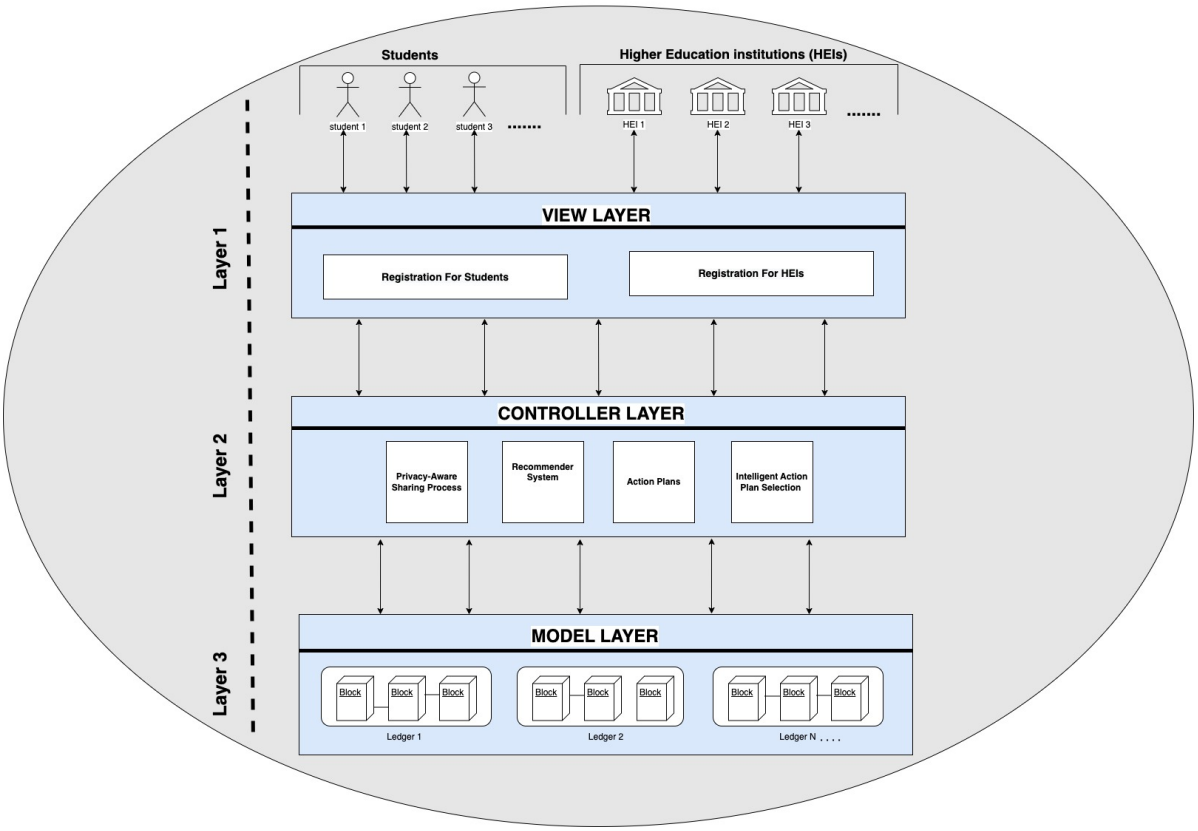

Figure 5.1: Architecture of the IBMM platform

5.2.1.1 View layer

This layer serves as the user interface (UI) for IBMM stakeholders, including students and HEIs. Through this layer, these stakeholders can engage with and access the platform actively as the owners of the data. In order to access the platform, both HEIs and students must register through this layer [17].
The HEIs have the ability to access and view the students' profiles and transfer completed

micro-credentials and action plans to be stored on the blockchain ledger through this layer. Furthermore, students themselves can access and view their profiles through this layer. Upon successful registration, both HEIs and students will be granted access to the requested data and will be authorized users. An overview of the main modules provided by the view layer is as follows:

1. **Registration for students:** In order for students to interact with the platform and access their micro-credentials and profiles on the IBMM platform, registration is required. Once students join the platform and their data is stored on the blockchain, a secure digital wallet will be created for them. This wallet includes a unique blockchain address, a public key, and a private key, to protect their data. A student also will be assigned a unique ID for identification purposes, which ensures the security and integrity of their data. A breakdown of how to register a student on the IBMM platform is as follows:

    - **Step 1:** Students visit the IBMM platform: To join the IBMM platform and interact with it, students are required to fill out a registration form with their information. The information includes personal details such as the student's name, date of birth, phone number, address, email address, etc.
    - **Step 2:** Students submit the registration form: After submitting the registration form, the information is securely transferred and stored in blocks on the blockchain ledger.
    - **Step 3:** Students are assigned secure digital wallets: Each newly registered student is assigned a unique, secure digital wallet with a blockchain address that includes a public key and a private key.
    - **Step 4:** Students are given student_IDs: Upon successful registration, every student is assigned a unique ID generated by the IBMM platform and stored on the blockchain.

2. **Registration for HEIs:** All higher education institutions, regardless of their type, location, and ownership, are eligible to become a member of the IBMM platform. Therefore, every higher education institution is able to join the IBMM by registering their information. Before being allowed to join the IBMM platform, each higher education institution must be officially approved and recognized by an accrediting body. The accrediting organization must confirm that the higher education institution has the necessary legal authority to operate as a higher

education institution and award higher education degrees [2].
Therefore, every higher education institution has to provide a unique identifier to prove that it is a legitimate institution. For example, Australia has a CRICOS code that is generated by "the Australian Government Department of Education" and shows the higher education institution adheres to standards, policies, and practices [43]. The CRICOS code is a unique identifier for a higher education institution and is used to verify that this higher education institution is real. Every country has a different identifier for its HEIs. When a higher education institution registers on the IBMM platform, they need to upload its unique identifier for verification by the minors. Once a higher education institution's registration is approved by majority consensus, it becomes a miner on the blockchain network.

5.2.1.2 Model layer

The model layer is also called the blockchain layer in the IBMM framework. It is a distributed database that stores and manages each completed transaction of the data, including micro-credentials [17]. Every completed transaction is stored on blocks in a secure, trusted, and private ledger. Blocks are constantly being added to an ever-growing chain of blocks called a ledger, and this chain is duplicated for every node of the network. This layer contains all the data logic in chaincode (smart contract) to simply manage and store the data [17]. The data that is stored on the blockchain ledger include a student's micro-credentials, academic records, student's personal information, and student's action plans. At this layer, the mining process verifies all the transactions on the blockchain. To develop this layer, we use the Hyperledger Fabric blockchain on the local device (Mac).

5.2.1.3 Controller layer

This layer functions as a connector between the view and model layers. Its responsibilities include receiving input from users, translating it into queries for the model layer, and controlling the presentation of data [17]. Additionally, this layer performs customized actions and implements various machine learning (ML) and artificial intelligence (AI) algorithms through pre-programmed smart contracts stored on the blockchain. These may include providing personalized recommendations to students about majors and action plans, etc [17].
As the IBMM is a trusted platform for managing and storing micro-credentials, the controller layer is responsible for controlling data flow, manipulation, integrity, and security via the use of algorithms. This layer comprises four modules, namely a privacy-

aware sharing process, a recommender system, action plans, and intelligent action plan selection and each provides a proposed solution for research questions RQ2-RQ4 detailed in this thesis. In the following, we describe each of these modules in detail:

- **Privacy-aware sharing process:** This module is designed for students who wish to maintain their anonymity when sharing their micro-credentials with several HEIs. The primary role of the privacy-aware sharing process is to ensure the confidentiality of students' information on the blockchain. To achieve objective 2, we use a privacy-preserving technique (PPT) called identity data anonymization, which utilizes cryptographic techniques. One of these techniques is the one-way hash function (SHA-256), which is applied to students' real identities to generate pseudonyms. This approach allows students to share their micro-credentials with HEIs using their pseudonyms while keeping their identities hidden. More details on this are given in Section 5.4.

- **Recommender system:** This module is utilized to assist students in determining the most suitable major based on their micro-credentials and academic achievements. In order to achieve objective 3 and provide personalized recommendations, an intelligent mechanism known as a recommender system (RS) is developed. The main role of this system is to intelligently recommend appropriate majors for students. The recommender system recommends a major for a student based on their micro-credentials, previous majors, and academic records. Further details are given in Chapter 6.

- **Action plans:** This module is used when students request action plans from multiple HEIs. To achieve objective 4, each action plan is generated by a different higher education institution and uploaded to the IBMM platform once HEIs receive a request from the student. Students can easily access all action plans that are offered by multiple HEIs and linked to their profiles through the IBMM platform. The goal is to provide students with a single view of all the action plans provided by several HEIs. Further details are given in Chapter 7.

- **Intelligent action plan selection:** This module assists students in selecting the most appropriate action plan from a variety of options. To achieve objective 4, an intelligent technique is used to select an appropriate action plan for a student based on their desired criteria. More details are given in Chapter 7.

5.2.2 IBMM platform stakeholders

The following tasks can be performed by the stakeholders, namely the students and HEIs, on the IBMM platform after successfully registering: Figure 5.2 provides an overview of the tasks for the end-users.

1. **Students:**
    - Accessing and viewing their profiles.
    - Viewing their stored micro-credentials.
    - Browsing through the list of registered HEIs.
    - Viewing the recommended majors that are generated for them.
    - Viewing all action plans provided by HEIs.
    - Viewing the suggested action plans that are generated for them.
2. **Higher Education Institution (HEIs):**
    - Accessing students' profiles using their IDs.
    - Uploading action plans for students after generating them.
    - Uploading students' micro-credentials after verifying them.
    - Viewing all students' micro-credentials and academic records that have been uploaded by other HEIs.

Section 5.3 provides details of how the first research question is addressed, followed by Section 5.4 which presents a detailed explanation of how the second research question is addressed.

5.3 Developing Hyperledger Fabric Blockchain Framework

This section explains the implementation of the proposed solution for the first research question, which is the development of a reliable and intelligent blockchain framework. The following subsections describe the steps involved in installing Hyperledger Fabric v2.x on a local device (MacOS), offering an insight into how the framework and chaincode (smart contracts) work together to store micro-credentials on a distributed ledger of a

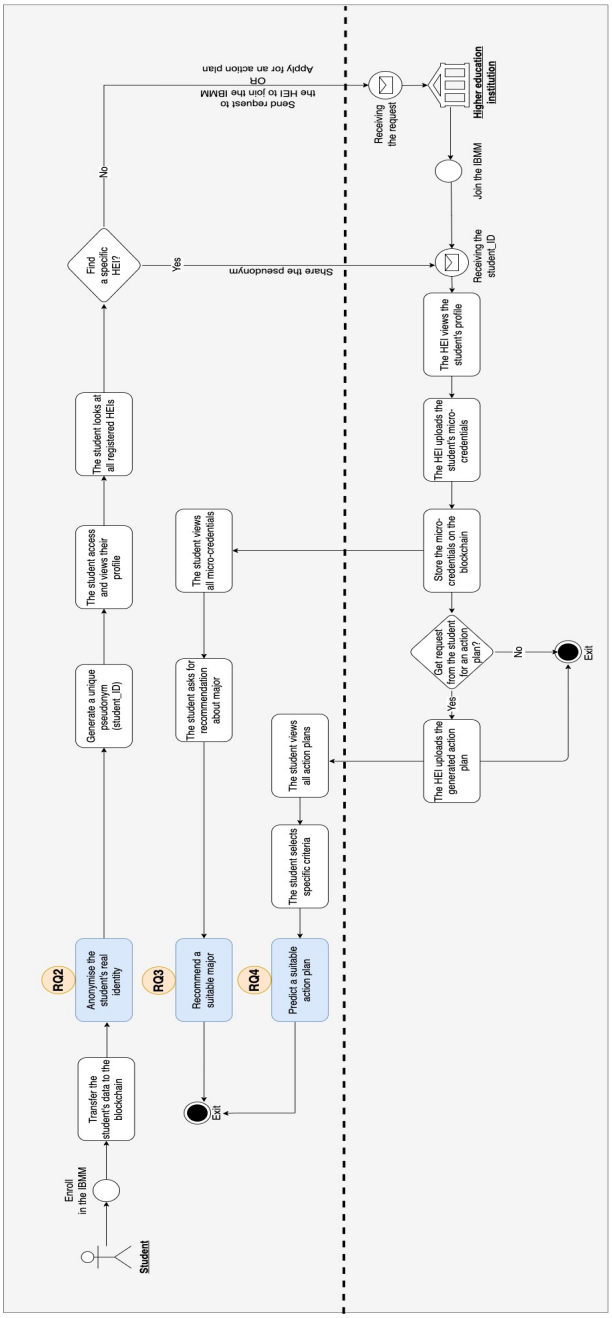

Figure 5.2: Overview of the tasks for the end-users

blockchain network. Furthermore, it elaborates on how to use APIs to invoke and query smart contracts through client applications and to interact with the Fabric network [5]. We utilize the TypeScript programming language (V5.2) to write the chaincode that executes specific contracts on peers and generates transactions for data accessibility and information storage [1].

Of the two types of peer-state databases supported by Fabric, we choose CouchDB. It is a separate database that runs in parallel with the peer [5]. With CouchDB, blockchain data is structured in JSON format, allowing extensive queries based on data values rather than keys [5]. The database also keeps track of the most recent ledger state. This database allows users to interact with chaincode and query large datasets more efficiently using JSON queries [5].

5.3.1 Standard prerequisite software for the Hyperledger Fabric network

Initially, the development environment and the required dependencies are set up to construct the network and application artifacts. To ensure compatibility, we first install the necessary prerequisites that match the MacOS version. It is necessary to install the following prerequisites in order to set up a fabric test network using Docker [5]:

- Install the following prerequisites fabric as shown in Table 5.1, using the scripts that are provided at Prerequisites [5].
- Install the fabric samples, fabric CLI tools binaries, and fabric docker images on the local machine (MacOS), using the commands and following the instructions that are provided at: Install Fabric and Fabric Samples [5].

5.3.2 The fabric test network

After all prerequisites have been installed and downloaded, a new fabric test network is set up as follows:

- First, we copy the fabric samples from [81]: hyperledger/fabric-samples, with v1.4.4 which is the latest version of the Fabric test network sample.
- Second, we navigate to test-network directory to run the network using the script found at: **"cd fabric-samples/test-network"** [81].
- Finally, we bring the Hyperledger Fabric network to our system by executing the script found at:**"./network.sh"** [5].
  To ensure a clean environment for the current run, we first execute the following script to eliminate any containers or artifacts from previous runs: **"./network.sh down"** as shown in Figure 5.5, and then we launch a new network by running the script found at **"./network.sh up"** as shown in Figures 5.6-5.17.

Table 5.1: The list of prerequisites

Prerequisites	**Description**
Homebrew	Homebrew version 3.6.15-23 is an open-source package management system that makes software installation on the Mac operating system easy [50].
Node js	Node js version 8.9.0 is an open-source server that is used to run JavaScript code [10].
Docker	Docker version 20.10.6 is a tool that simplifies the process of developing, distributing, and running applications within virtual containers [6].
Xcode Command Line Tools	Xcode CLT version 2.12.7 is a tool operated through the command-line interface, enabling users to execute build, query, analyze, and test operations on Xcode projects and workspaces. It is also called a console or terminal [90].
jq	jq-1.6 is a JSON processor that is used through the command-line interface and it allows users to view a JSON file [22].
Go	Go version 1.15.6 is a programming language that is used to write Chaincode or SDK applications [5].
cURL	Curl version 7.74.0 is a tool for transmitting data via the internet [80].
Git	Git version 2.31.0 is a control system to keep track of the changes made in source code, enabling collaboration between multiple developers on non-linear development projects [75].
Docker Compose	Docker-compose version 1.29.1 is a tool specifically designed for the management of Docker applications with multiple containers [6].

Once the test network is successfully created, all the Docker containers and the logs of the nodes that have been running and were created on our machine can be seen using the script at **"docker ps -a"** as shown in Figure 5.18. The network that runs on our machine contains 2 peer organizations, Org1 and Org2, 4 peer nodes and each node or user needs to be a member of one organization to be a part of the network, one ordering node, and 2 Fabric Certificate Authorities (CAs) for the organizations. Peer nodes do not control the order of transactions or include them in new blocks; instead, they validate the transactions and assign them to the blockchain ledger. The ordering node is responsible for arranging transactions, including them into blocks, and distributing the blocks to peer nodes to add them to the ledger [5].

5.3.3 The sample application

Once peer and orderer nodes are running successfully on our machine, the sample application can be launched using the following steps:

- Create a fabric channel: We create a channel as a private layer for the communication and transactions between Org1 and Org2. Each channel has a copy of the blockchain ledger. We execute the following script: **"./network.sh up createChannel -ca -c mychannel -s couchdb"** [5]. This script is used to create a channel called *"mychannel"* with two peer organizations and one ordering node and bring up the network in one step, and join Org1 and Org2 are joined to this channel as shown in Figures 5.6-5.17. Figure 5.3 shows the printed message that confirms the channel was successfully created.

```
Status: 201
{
        "name": "mychannel",
        "url": "/participation/v1/channels/mychannel",
        "consensusRelation": "consenter",
        "status": "active",
        "height": 1
}

Channel 'mychannel' created
```

Figure 5.3: The message confirming the channel was created successfully

- Start a chaincode on the channel: Once the channel is successfully established, smart contracts (chaincode) can be used to communicate with the channel. chaincode packages are used to implement smart contracts on the network. chaincode must first be placed on the peers of an organization and the channel's participants must agree on the chaincode specification before it can be deployed to the channel. The chaincode is ready to use and can be submitted to the channel when the majority of organizations agree on it [5].
  The chaincode is developed by creating smart contracts that can perform many functions including but not limited to enrolling students and HEIs, adding micro-credentials, and viewing students' profiles, etc. The original code of the chaincode can be found on GitHub at: `https://github.com/hyperledger/fabric-samples/blob/main/asset-transfer-basic/chaincode-typescript/src/assetTransfer.ts`. Our developed code for the chaincode can be found on GitHub at: `https://github.com/hudaalsobhi/IBMM-code.git`
  After creating the channel, the chaincode is deployed using the script at: **"./network.sh deployCC -ccn basic -ccp ../credit-transfer-basic/chaincode-typescript -ccl typescript"** [5] as shown in Figures 5.19 - 5.22.
  To ensure the transactions that are generated using smart contracts are valid, the consensus algorithm often requires several organizations to sign them before they can be committed to the blockchain ledger [5]. Every organization must invoke and implement the smart contract on their peer to sign a transaction, and the peer then signs the transaction's output. The transaction can be added to the blockchain ledger if the transaction's output is accurate and has been signed by an adequate number of organizations [5].

- Setup the environment variables: We add peer binaries to the CLI path, set the fabric path, and set the environment variables to allow the use of the peer CLI to interact with the network. We use the following scripts at V3 [5]:

  - "export PATH=$PWD/../bin:$PATH"
  - "export FABRIC_CFG_PATH=$PWD/../config/"
  - "export CORE_PEER_TLS_ENABLED=true"
  - "export CORE_PEER_LOCALMSPID="Org1MSP""
  - "export CORE_PEER_TLS_ROOTCERT_FILE=$PWD/organizations /peerOrganizations/org1.example.com/peers/peer0.org1.example.com/tls/ca.crt"

  - "export CORE_PEER_MSPCONFIGPATH= $PWD/organizations/peerOrganizations/org1.example.com/users/Admin@org1.example.com/msp"
  - "export CORE_PEER_ADDRESS=localhost:7051"

- Interacting with the network: After we bring up the network, we invoke our typescript chaincode to interact with this network as shown in Figure 5.23. We use the following script to initialize the ledger [5]:

  "peer chaincode invoke -o localhost:7050 –ordererTLSHostnameOverride orderer.example.com–tls –cafile "$PWD/organizations/ordererOrganizations /example.com/orderers/orderer.example.com/msp/tlscacerts/tlsca.example.com-cert.pem" -C mychannel -n basic –peerAddresses localhost:7051 –tlsRootCertFiles "$PWD/organizations/peerOrganizations/org1.example.com/peers/peer0.org1.example.com/tls/ca.crt" –peerAddresses localhost:9051 –tlsRootCertFiles "$PWD/organizations/peerOrganizations/org2.example.com/peers/peer0.org2.example.com/tls/ca.crt" -c '{"function":"InitLedger","Args":[]'}".

Once all the previous steps have been successfully completed and the chaincode has been invoked, we query the ledger locally from our CLI. Every time a modification is made to the chaincode by the network members or new data is transferred, we need to invoke the chaincode again. A subsequent query can then be conducted to observe how the invocation has affected the data on the ledger [5].

The following Section 5.4 presents the proposed solution for the second research question in detail. Section 5.6, presents the evaluation process for the HyperLedger Fabric blockchain application and for the privacy-aware sharing process. This allows us to engage with the blockchain network and chaincode, effectively achieving the primary objectives of this research.

5.4 A Blockchain-based Approach to Ensure Privacy and Data Preservation for Students

This section addresses the second research question regarding privacy preservation and provides a blockchain-based approach to securely preserve students' data on the blockchain within the IBMM. The proposed approach is designed to promote privacy in the context of students' data, providing a framework for the permanent retention of

important data. To achieve objective 2, an effective technique for maintaining students' real identities on the blockchain is implemented. The IBMM platform helps to protect students' real identities while sharing their profiles and micro-credentials with other HEIs. This ensures that there is no possibility of disclosing a student's real identity within the IBMM platform. To enable the anonymous searchability of student data within the IBMM platform, a cryptographic hashing technique that assigns a unique pseudonym to every student is applied.
Due to blockchain's immutability and secure encryption of data on blocks, blockchain technology is highly resistant to cyberattacks [93]. Additionally, to further enhance privacy and ensure anonymity for students, a pseudonymization technique is also used which replaces a student's identity with a pseudonym to preserve the anonymity of students as explained in the following section.

5.5 Solution Overview for Preserving Student Privacy during Data Sharing

The second research question of this thesis addresses how micro-credentials can be shared while ensuring student data privacy and the need to protect the anonymity of student identities when their profiles and micro-credentials are shared with HEIs. This section describes the privacy-aware sharing process as the proposed solution for RQ2 which is ***How can micro-credentials be shared taking into account the student's privacy?***. A detailed explanation is given of the privacy-preserving technique that is implemented with the Hyperledger Fabric blockchain to generate pseudonyms for students.

To ensure the privacy of students' data and the anonymity of their identities, the SHA-2 algorithm, which includes several constants, with SHA-256 being one of them, is selected for this experiment. The output size of SHA-256 is a fixed-size 256 bits, which generates a distinct output of 2^{256}. A hashing approach ensures that a student's real identity remains hidden from view, making it difficult for HEIs to identify the student. We use **a one-way hash function (SHA-256)** to keep students' real identities anonymous and replace them with hash values, known as pseudonyms in this research. Consequently, the student's identity remains anonymous, preserving the privacy of the students while allowing them to interact with the blockchain network through the IBMM platform and verify its integrity when necessary.

The smart contract logic for applying the SHA-256 hash function is written in the TypeScript programming language using the Hyperledger Fabric SDKs. The software development kit (SDK) supports the execution of smart contracts in various programming languages, such as Java, JavaScript, TypeScript, Python, and GO [5]. The outcomes of utilizing the one-way hash function (SHA-256) to generate pseudonyms for students and ensure privacy are depicted in Figures 5.35 and 5.36. Figure 5.4 shows the workflow of generating a pseudonym. The steps involved in generating a unique pseudonym for a student using the hashing algorithm are presented in Chapter 4 in Section 4.3.2.

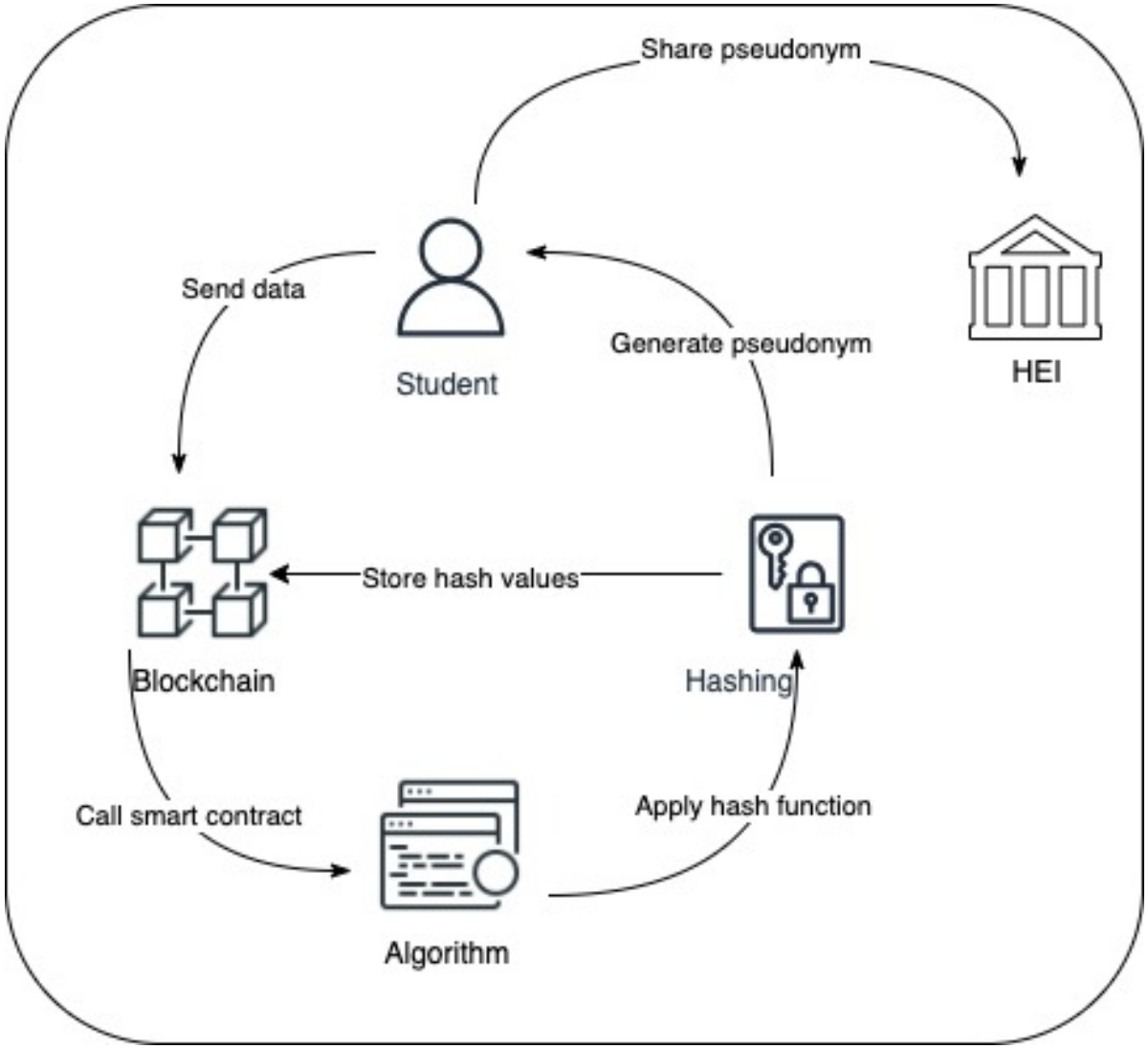

Figure 5.4: The process of generating pseudonyms

The process begins with a student registering on the IBMM platform by providing all

their personal information, including their name, date of birth, address, phone number, and email address. This information is then transferred onto the ledger to be stored on the blockchain. The chaincode needs to be invoked every time a new student is added to the ledger. Then, the smart contract that is responsible for executing the hash algorithm (SHA-256) is implemented only on specific data, such as the student's name and email address. We chose only these data to be anonymized because they serve as identifiers for the student and can be used to reveal the student's real identity. Therefore, anonymization is essential to prevent the disclosure of the student's real identity and preserve their privacy. Once the hash algorithm (SHA-256) is implemented successfully to both the student's name and email address, two different hash values are generated for each of the data separately. Furthermore, the hash function helps to anonymize the real identity of the students by hashing the student's name and email address. These hash values serve to represent the student's real identity in a unique and anonymous manner, protecting the student's data while securely facilitating micro-credential management and verification on the IBMM platform.

Next, we combine the hash values obtained for both the student's name and email address, and this combined output is subjected again to the SHA-256 algorithm to generate a unique pseudonym. By using this process, every student is assigned a unique ID which is their pseudonym to be shared with multiple HEIs off-chain to facilitate access to their profiles and micro-credentials. Using this pseudonym, HEIs can access the student's profile and read their micro-credentials that are stored on the blockchain ledger securely and anonymously without compromising the student's real identity.

Finally, the transaction outputs are signed by multiple organizations and stored on the blockchain ledger. This process ensures that the data is secure, tamper-proof, and cannot be changed in any way without being detected. It also ensures the anonymity of the student's identity and prevents their real name and email address from being disclosed to HEIs during the interaction with the IBMM platform. Furthermore, by replacing the real identity of the student with a pseudonym, the student's privacy is protected, and their anonymity is maintained throughout the entire process. The use of a pseudonym generated by the hash algorithm ensures that the student's identity remains protected while sharing their micro-credentials with HEIs. The student pseudonym provides a secure way for HEIs to access the student's micro-credentials and profile without compromising their privacy.

5.6 Prototype Evaluation and Discussion

This section presents the validation process of the proposed solutions of RQ1 and RQ2. The purpose of this evaluation is to measure both the effectiveness of developing the Hyperledger Fabric blockchain framework and implementing the privacy-preserving method.

5.6.1 Validation process for developing the Hyperledger Fabric blockchain

This section explains how to validate the development of the Hyperledger Fabric blockchain network that is used to build the IBMM platform. We are able to query and invoke the chaincode through our CLI (command-line interface) using specific commands.
After all the prerequisites described in Section 5.3.1 have been installed on our device (MacOS) and the required version of the hyperledger/fabric-samples has been cloned, the following steps are followed to install the HyperLedger Fabric network:

1. We bring down the network to stop and remove chaincode containers, images, or channel artifacts from previous runs. Figure 5.5 shows the outcome of running this command: **./network.sh down**.

```
hudaalsobhi@192-168-1-164 ~/OneDrive/Blockchain-workspace/IBMM-workspace/blockchain/blockchain_credentials/australia_education_project/fabric-samples/test-network % ./network.sh down

Using docker and docker-compose
Stopping network
Stopping cli                    ... done
Stopping peer0.org1.example.com ... done
Stopping peer0.org2.example.com ... done
Stopping orderer.example.com    ... done
Stopping couchdb1               ... done
Stopping couchdb0               ... done
Stopping ca_org1                ... done
Stopping ca_org2                ... done
Stopping ca_orderer             ... done
Removing cli                    ... done
Removing peer0.org1.example.com ... done
Removing peer0.org2.example.com ... done
Removing orderer.example.com    ... done
Removing couchdb1               ... done
Removing couchdb0               ... done
Removing ca_org1                ... done
Removing ca_org2                ... done
Removing ca_orderer             ... done
Removing network fabric_test
Removing network compose_default
WARNING: Network compose_default not found.
Removing volume compose_orderer.example.com
Removing volume compose_peer0.org1.example.com
Removing volume compose_peer0.org2.example.com
Removing volume compose_peer0.org3.example.com
WARNING: Volume compose_peer0.org3.example.com not found.
Error: No such volume: docker_orderer.example.com
Error: No such volume: docker_peer0.org1.example.com
Error: No such volume: docker_peer0.org2.example.com
Removing remaining containers
Removing generated chaincode docker images
Untagged: dev-peer0.org2.example.com-basic_1.0-af3227795a66b828e7eafa47cbd12376dc2da371a1971b27fe58bddfa773a698-6e5df044ba4ef87af7832f33b52a5de71dcf3903b72e2b0eb498cac697587ffd:latest
Deleted: sha256:2b7edb46ed8c142cfeeeff410df17bc92029d0d5b04b1559ff12cca00a79f2e3
Deleted: sha256:af8b1a761324705d77b804b8a87dc22459abddc19f03fef67fe321868fcfc2d2
Deleted: sha256:1a6c48b00905506319f4c3f5e8eb2d8b23b4fc863659604a8ad2432a9aaf2e40
Deleted: sha256:00e6f8fda6f37d84dc6d66444785c166154a26679da10332089e26bb0fde1cce
Untagged: dev-peer0.org1.example.com-basic_1.0-af3227795a66b828e7eafa47cbd12376dc2da371a1971b27fe58bddfa773a698-962197022f9d608718f237cf84b73e603f319c50e2dbeae355fb6c2683da55af:latest
Deleted: sha256:426b23a3ce1bf370b2d1bdf6c6a66b12bc400ff95312926776 5e669de005b382
Deleted: sha256:dfec947e9d0ccb2dd765232d73279d27c72b8dd675d1f40a154fbbc57b631e85
Deleted: sha256:f842beb23063e008bc78269be035cd2eccb5c865a2b99a592c295502a7c867fa
Deleted: sha256:a8b571ffaef027455caf19efb8164e0183e34706e571cb94e3958b33267e88d6
"docker kill" requires at least 1 argument.
See 'docker kill --help'.
```

Figure 5.5: Bringing down the network

2. We bring up the network and establish a channel in one step. As illustrated in Figures 5.6 - 5.17, a Fabric network comprising an ordering node and two peer nodes has been established. Furthermore, a Fabric channel has also been created to enable peer nodes to join the channel and facilitate communication between Org1 and Org2.

```
hudaalsobhi@192-168-1-164 ~/OneDrive/Blockchain-workspace/IBMM-workspace/blockchain/blockchain_credentials/australia_education_project/fabric-samples/test-netw
ork % ./network.sh up createChannel -ca -c mychannel -s couchdb

Using docker and docker-compose
Creating channel 'mychannel'.
If network is not up, starting nodes with CLI timeout of '5' tries and CLI delay of '3' seconds and using database 'couchdb with crypto from 'Certificate Autho
rities'
Bringing up network
LOCAL_VERSION=2.2.1
DOCKER_IMAGE_VERSION=2.4.7
Local fabric binaries and docker images are out of  sync. This may cause problems.
CA_LOCAL_VERSION=1.5.5
CA_DOCKER_IMAGE_VERSION=1.5.5
Generating certificates using Fabric CA
Docker Compose is now in the Docker CLI, try `docker compose up`

Creating network "fabric_test" with the default driver
Creating ca_orderer ... done
Creating ca_org1    ... done
Creating ca_org2    ... done
Creating Org1 Identities
Enrolling the CA admin
+ fabric-ca-client enroll -u https://admin:adminpw@localhost:7054 --caname ca-org1 --tls.certfiles /Users/hudaalsobhi/OneDrive/Blockchain-workspace/IBMM-worksp
ace/blockchain/blockchain_credentials/australia_education_project/fabric-samples/test-network/organizations/fabric-ca/org1/ca-cert.pem
2023/07/21 15:49:25 [INFO] Created a default configuration file at /Users/hudaalsobhi/OneDrive/Blockchain-workspace/IBMM-workspace/blockchain/blockchain_creden
tials/australia_education_project/fabric-samples/test-network/organizations/peerOrganizations/org1.example.com/fabric-ca-client-config.yaml
2023/07/21 15:49:25 [INFO] TLS Enabled
2023/07/21 15:49:25 [INFO] generating key: &{A:ecdsa S:256}
2023/07/21 15:49:25 [INFO] encoded CSR
2023/07/21 15:49:25 [INFO] Stored client certificate at /Users/hudaalsobhi/OneDrive/Blockchain-workspace/IBMM-workspace/blockchain/blockchain_credentials/austr
alia_education_project/fabric-samples/test-network/organizations/peerOrganizations/org1.example.com/msp/signcerts/cert.pem
2023/07/21 15:49:25 [INFO] Stored root CA certificate at /Users/hudaalsobhi/OneDrive/Blockchain-workspace/IBMM-workspace/blockchain/blockchain_credentials/aust
ralia_education_project/fabric-samples/test-network/organizations/peerOrganizations/org1.example.com/msp/cacerts/localhost-7054-ca-org1.pem
2023/07/21 15:49:25 [INFO] Stored Issuer public key at /Users/hudaalsobhi/OneDrive/Blockchain-workspace/IBMM-workspace/blockchain/blockchain_credentials/austra
lia_education_project/fabric-samples/test-network/organizations/peerOrganizations/org1.example.com/msp/IssuerPublicKey
2023/07/21 15:49:25 [INFO] Stored Issuer revocation public key at /Users/hudaalsobhi/OneDrive/Blockchain-workspace/IBMM-workspace/blockchain/blockchain_credent
ials/australia_education_project/fabric-samples/test-network/organizations/peerOrganizations/org1.example.com/msp/IssuerRevocationPublicKey
Registering peer0
+ fabric-ca-client register --caname ca-org1 --id.name peer0 --id.secret peer0pw --id.type peer --tls.certfiles /Users/hudaalsobhi/OneDrive/Blockchain-workspac
e/IBMM-workspace/blockchain/blockchain_credentials/australia_education_project/fabric-samples/test-network/organizations/fabric-ca/org1/ca-cert.pem
2023/07/21 15:49:25 [INFO] Configuration file location: /Users/hudaalsobhi/OneDrive/Blockchain-workspace/IBMM-workspace/blockchain/blockchain_credentials/austr
alia_education_project/fabric-samples/test-network/organizations/peerOrganizations/org1.example.com/fabric-ca-client-config.yaml
2023/07/21 15:49:25 [INFO] TLS Enabled
```

Figure 5.6: Bringing up the network and creating a channel (1st figure of 12)

After the network has been created successfully, its components can be displayed. Figure 5.18 shows the Docker containers that are running on the machine.

3. We deploy the chaincode on the channel. Figures 5.19 - 5.22 illustrate that the chaincode is installed on an organization's peer nodes, and subsequently deployed to the channel.

4. We invoke the chaincode to initialize the ledger. If the invoke goes successfully, we see an output similar to this in Figure 5.23.

5. By querying the ledger, members can now actively engage with the channel. To complete the tasks previously outlined for both students and HEIs in Section 5.2, the following commands must be executed via the CLI:

```
Password: peer0pw
Registering user
+ fabric-ca-client register --caname ca-org1 --id.name user1 --id.secret user1pw --id.type client --tls.certfiles /Users/hudaalsobhi/OneDrive/Blockchain-worksp
ace/IBMM-workspace/blockchain/blockchain_credentials/australia_education_project/fabric-samples/test-network/organizations/fabric-ca/org1/ca-cert.pem
2023/07/21 15:49:25 [INFO] Configuration file location: /Users/hudaalsobhi/OneDrive/Blockchain-workspace/IBMM-workspace/blockchain/blockchain_credentials/austr
alia_education_project/fabric-samples/test-network/organizations/peerOrganizations/org1.example.com/fabric-ca-client-config.yaml
2023/07/21 15:49:25 [INFO] TLS Enabled
2023/07/21 15:49:25 [INFO] TLS Enabled
Password: user1pw
Registering the org admin
+ fabric-ca-client register --caname ca-org1 --id.name org1admin --id.secret org1adminpw --id.type admin --tls.certfiles /Users/hudaalsobhi/OneDrive/Blockchain
-workspace/IBMM-workspace/blockchain/blockchain_credentials/australia_education_project/fabric-samples/test-network/organizations/fabric-ca/org1/ca-cert.pem
2023/07/21 15:49:25 [INFO] Configuration file location: /Users/hudaalsobhi/OneDrive/Blockchain-workspace/IBMM-workspace/blockchain/blockchain_credentials/austr
alia_education_project/fabric-samples/test-network/organizations/peerOrganizations/org1.example.com/fabric-ca-client-config.yaml
2023/07/21 15:49:25 [INFO] TLS Enabled
2023/07/21 15:49:25 [INFO] TLS Enabled
Password: org1adminpw
Generating the peer0 msp
+ fabric-ca-client enroll -u https://peer0:peer0pw@localhost:7054 --caname ca-org1 -M /Users/hudaalsobhi/OneDrive/Blockchain-workspace/IBMM-workspace/blockchai
n/blockchain_credentials/australia_education_project/fabric-samples/test-network/organizations/peerOrganizations/org1.example.com/peers/peer0.org1.example.com/
msp --csr.hosts peer0.org1.example.com --tls.certfiles /Users/hudaalsobhi/OneDrive/Blockchain-workspace/IBMM-workspace/blockchain/blockchain_credentials/austra
lia_education_project/fabric-samples/test-network/organizations/fabric-ca/org1/ca-cert.pem
2023/07/21 15:49:25 [INFO] TLS Enabled
2023/07/21 15:49:25 [INFO] generating key: &{A:ecdsa S:256}
2023/07/21 15:49:25 [INFO] encoded CSR
2023/07/21 15:49:25 [INFO] Stored client certificate at /Users/hudaalsobhi/OneDrive/Blockchain-workspace/IBMM-workspace/blockchain/blockchain_credentials/austr
alia_education_project/fabric-samples/test-network/organizations/peerOrganizations/org1.example.com/peers/peer0.org1.example.com/msp/signcerts/cert.pem
2023/07/21 15:49:25 [INFO] Stored root CA certificate at /Users/hudaalsobhi/OneDrive/Blockchain-workspace/IBMM-workspace/blockchain/blockchain_credentials/aust
ralia_education_project/fabric-samples/test-network/organizations/peerOrganizations/org1.example.com/peers/peer0.org1.example.com/msp/cacerts/localhost-7054-ca
-org1.pem
2023/07/21 15:49:25 [INFO] Stored Issuer public key at /Users/hudaalsobhi/OneDrive/Blockchain-workspace/IBMM-workspace/blockchain/blockchain_credentials/austra
lia_education_project/fabric-samples/test-network/organizations/peerOrganizations/org1.example.com/peers/peer0.org1.example.com/msp/IssuerPublicKey
2023/07/21 15:49:25 [INFO] Stored Issuer revocation public key at /Users/hudaalsobhi/OneDrive/Blockchain-workspace/IBMM-workspace/blockchain/blockchain_credent
ials/australia_education_project/fabric-samples/test-network/organizations/peerOrganizations/org1.example.com/peers/peer0.org1.example.com/msp/IssuerRevocation
PublicKey
Generating the peer0-tls certificates
+ fabric-ca-client enroll -u https://peer0:peer0pw@localhost:7054 --caname ca-org1 -M /Users/hudaalsobhi/OneDrive/Blockchain-workspace/IBMM-workspace/blockchai
n/blockchain_credentials/australia_education_project/fabric-samples/test-network/organizations/peerOrganizations/org1.example.com/peers/peer0.org1.example.com/
tls --enrollment.profile tls --csr.hosts peer0.org1.example.com --csr.hosts localhost --tls.certfiles /Users/hudaalsobhi/OneDrive/Blockchain-workspace/IBMM-wor
kspace/blockchain/blockchain_credentials/australia_education_project/fabric-samples/test-network/organizations/fabric-ca/org1/ca-cert.pem
2023/07/21 15:49:26 [INFO] TLS Enabled
2023/07/21 15:49:26 [INFO] generating key: &{A:ecdsa S:256}
2023/07/21 15:49:26 [INFO] encoded CSR
```

Figure 5.7: Bringing up the network and creating a channel (2nd figure of 12)

```
2023/07/21 15:49:26 [INFO] Stored client certificate at /Users/hudaalsobhi/OneDrive/Blockchain-workspace/IBMM-workspace/blockchain/blockchain_credentials/austr
alia_education_project/fabric-samples/test-network/organizations/peerOrganizations/org1.example.com/peers/peer0.org1.example.com/tls/signcerts/cert.pem
2023/07/21 15:49:26 [INFO] Stored TLS root CA certificate at /Users/hudaalsobhi/OneDrive/Blockchain-workspace/IBMM-workspace/blockchain/blockchain_credentials/
australia_education_project/fabric-samples/test-network/organizations/peerOrganizations/org1.example.com/peers/peer0.org1.example.com/tls/tlscacerts/tls-localh
ost-7054-ca-org1.pem
2023/07/21 15:49:26 [INFO] Stored Issuer public key at /Users/hudaalsobhi/OneDrive/Blockchain-workspace/IBMM-workspace/blockchain/blockchain_credentials/austra
lia_education_project/fabric-samples/test-network/organizations/peerOrganizations/org1.example.com/peers/peer0.org1.example.com/tls/IssuerPublicKey
2023/07/21 15:49:26 [INFO] Stored Issuer revocation public key at /Users/hudaalsobhi/OneDrive/Blockchain-workspace/IBMM-workspace/blockchain/blockchain_credent
ials/australia_education_project/fabric-samples/test-network/organizations/peerOrganizations/org1.example.com/peers/peer0.org1.example.com/tls/IssuerRevocation
PublicKey
Generating the user msp
+ fabric-ca-client enroll -u https://user1:user1pw@localhost:7054 --caname ca-org1 -M /Users/hudaalsobhi/OneDrive/Blockchain-workspace/IBMM-workspace/blockchai
n/blockchain_credentials/australia_education_project/fabric-samples/test-network/organizations/peerOrganizations/org1.example.com/users/User1@org1.example.com/
msp --tls.certfiles /Users/hudaalsobhi/OneDrive/Blockchain-workspace/IBMM-workspace/blockchain/blockchain_credentials/australia_education_project/fabric-sample
s/test-network/organizations/fabric-ca/org1/ca-cert.pem
2023/07/21 15:49:26 [INFO] TLS Enabled
2023/07/21 15:49:26 [INFO] generating key: &{A:ecdsa S:256}
2023/07/21 15:49:26 [INFO] encoded CSR
2023/07/21 15:49:26 [INFO] Stored client certificate at /Users/hudaalsobhi/OneDrive/Blockchain-workspace/IBMM-workspace/blockchain/blockchain_credentials/austr
alia_education_project/fabric-samples/test-network/organizations/peerOrganizations/org1.example.com/users/User1@org1.example.com/msp/signcerts/cert.pem
2023/07/21 15:49:26 [INFO] Stored root CA certificate at /Users/hudaalsobhi/OneDrive/Blockchain-workspace/IBMM-workspace/blockchain/blockchain_credentials/aust
ralia_education_project/fabric-samples/test-network/organizations/peerOrganizations/org1.example.com/users/User1@org1.example.com/msp/cacerts/localhost-7054-ca
-org1.pem
2023/07/21 15:49:26 [INFO] Stored Issuer public key at /Users/hudaalsobhi/OneDrive/Blockchain-workspace/IBMM-workspace/blockchain/blockchain_credentials/austra
lia_education_project/fabric-samples/test-network/organizations/peerOrganizations/org1.example.com/users/User1@org1.example.com/msp/IssuerPublicKey
2023/07/21 15:49:26 [INFO] Stored Issuer revocation public key at /Users/hudaalsobhi/OneDrive/Blockchain-workspace/IBMM-workspace/blockchain/blockchain_credent
ials/australia_education_project/fabric-samples/test-network/organizations/peerOrganizations/org1.example.com/users/User1@org1.example.com/msp/IssuerRevocation
PublicKey
Generating the org admin msp
+ fabric-ca-client enroll -u https://org1admin:org1adminpw@localhost:7054 --caname ca-org1 -M /Users/hudaalsobhi/OneDrive/Blockchain-workspace/IBMM-workspace/b
lockchain/blockchain_credentials/australia_education_project/fabric-samples/test-network/organizations/peerOrganizations/org1.example.com/users/Admin@org1.exam
ple.com/msp --tls.certfiles /Users/hudaalsobhi/OneDrive/Blockchain-workspace/IBMM-workspace/blockchain/blockchain_credentials/australia_education_project/fabri
c-samples/test-network/organizations/fabric-ca/org1/ca-cert.pem
2023/07/21 15:49:26 [INFO] TLS Enabled
2023/07/21 15:49:26 [INFO] generating key: &{A:ecdsa S:256}
2023/07/21 15:49:26 [INFO] encoded CSR
2023/07/21 15:49:26 [INFO] Stored client certificate at /Users/hudaalsobhi/OneDrive/Blockchain-workspace/IBMM-workspace/blockchain/blockchain_credentials/austr
alia_education_project/fabric-samples/test-network/organizations/peerOrganizations/org1.example.com/users/Admin@org1.example.com/msp/signcerts/cert.pem
2023/07/21 15:49:26 [INFO] Stored root CA certificate at /Users/hudaalsobhi/OneDrive/Blockchain-workspace/IBMM-workspace/blockchain/blockchain_credentials/aust
ralia_education_project/fabric-samples/test-network/organizations/peerOrganizations/org1.example.com/users/Admin@org1.example.com/msp/cacerts/localhost-7054-ca
-org1.pem
2023/07/21 15:49:26 [INFO] Stored Issuer public key at /Users/hudaalsobhi/OneDrive/Blockchain-workspace/IBMM-workspace/blockchain/blockchain_credentials/austra
lia_education_project/fabric-samples/test-network/organizations/peerOrganizations/org1.example.com/users/Admin@org1.example.com/msp/IssuerPublicKey
```

Figure 5.8: Bringing up the network and creating a channel (3rd figure of 12)

- Get all students' profiles that are stored on the blockchain ledger: Figure 5.24 shows the profiles of two students who have already registered using the "GetAllStudents" function, including their personal information, micro-credentials, and action plans.

```
2023/07/21 15:49:26 [INFO] Stored Issuer revocation public key at /Users/hudaalsobhi/OneDrive/Blockchain-workspace/IBMM-workspace/blockchain/blockchain_credent
ials/australia_education_project/fabric-samples/test-network/organizations/peerOrganizations/org1.example.com/users/Admin@org1.example.com/msp/IssuerRevocation
PublicKey
Creating Org2 Identities
Enrolling the CA admin
+ fabric-ca-client enroll -u https://admin:adminpw@localhost:8054 --caname ca-org2 --tls.certfiles /Users/hudaalsobhi/OneDrive/Blockchain-workspace/IBMM-worksp
ace/blockchain/blockchain_credentials/australia_education_project/fabric-samples/test-network/organizations/fabric-ca/org2/ca-cert.pem
2023/07/21 15:49:26 [INFO] Created a default configuration file at /Users/hudaalsobhi/OneDrive/Blockchain-workspace/IBMM-workspace/blockchain/blockchain_creden
tials/australia_education_project/fabric-samples/test-network/organizations/peerOrganizations/org2.example.com/fabric-ca-client-config.yaml
2023/07/21 15:49:26 [INFO] TLS Enabled
2023/07/21 15:49:26 [INFO] generating key: &{A:ecdsa S:256}
2023/07/21 15:49:26 [INFO] encoded CSR
2023/07/21 15:49:26 [INFO] Stored client certificate at /Users/hudaalsobhi/OneDrive/Blockchain-workspace/IBMM-workspace/blockchain/blockchain_credentials/austr
alia_education_project/fabric-samples/test-network/organizations/peerOrganizations/org2.example.com/msp/signcerts/cert.pem
2023/07/21 15:49:26 [INFO] Stored root CA certificate at /Users/hudaalsobhi/OneDrive/Blockchain-workspace/IBMM-workspace/blockchain/blockchain_credentials/aust
ralia_education_project/fabric-samples/test-network/organizations/peerOrganizations/org2.example.com/msp/cacerts/localhost-8054-ca-org2.pem
2023/07/21 15:49:26 [INFO] Stored Issuer public key at /Users/hudaalsobhi/OneDrive/Blockchain-workspace/IBMM-workspace/blockchain/blockchain_credentials/austra
lia_education_project/fabric-samples/test-network/organizations/peerOrganizations/org2.example.com/msp/IssuerPublicKey
2023/07/21 15:49:26 [INFO] Stored Issuer revocation public key at /Users/hudaalsobhi/OneDrive/Blockchain-workspace/IBMM-workspace/blockchain/blockchain_credent
ials/australia_education_project/fabric-samples/test-network/organizations/peerOrganizations/org2.example.com/msp/IssuerRevocationPublicKey
Registering peer0
+ fabric-ca-client register --caname ca-org2 --id.name peer0 --id.secret peer0pw --id.type peer --tls.certfiles /Users/hudaalsobhi/OneDrive/Blockchain-workspac
e/IBMM-workspace/blockchain/blockchain_credentials/australia_education_project/fabric-samples/test-network/organizations/fabric-ca/org2/ca-cert.pem
2023/07/21 15:49:26 [INFO] Configuration file location: /Users/hudaalsobhi/OneDrive/Blockchain-workspace/IBMM-workspace/blockchain/blockchain_credentials/austr
alia_education_project/fabric-samples/test-network/organizations/peerOrganizations/org2.example.com/fabric-ca-client-config.yaml
2023/07/21 15:49:26 [INFO] TLS Enabled
2023/07/21 15:49:26 [INFO] TLS Enabled
Password: peer0pw
Registering user
+ fabric-ca-client register --caname ca-org2 --id.name user1 --id.secret user1pw --id.type client --tls.certfiles /Users/hudaalsobhi/OneDrive/Blockchain-worksp
ace/IBMM-workspace/blockchain/blockchain_credentials/australia_education_project/fabric-samples/test-network/organizations/fabric-ca/org2/ca-cert.pem
2023/07/21 15:49:26 [INFO] Configuration file location: /Users/hudaalsobhi/OneDrive/Blockchain-workspace/IBMM-workspace/blockchain/blockchain_credentials/austr
alia_education_project/fabric-samples/test-network/organizations/peerOrganizations/org2.example.com/fabric-ca-client-config.yaml
2023/07/21 15:49:26 [INFO] TLS Enabled
2023/07/21 15:49:26 [INFO] TLS Enabled
Password: user1pw
Registering the org admin
+ fabric-ca-client register --caname ca-org2 --id.name org2admin --id.secret org2adminpw --id.type admin --tls.certfiles /Users/hudaalsobhi/OneDrive/Blockchain
-workspace/IBMM-workspace/blockchain/blockchain_credentials/australia_education_project/fabric-samples/test-network/organizations/fabric-ca/org2/ca-cert.pem
2023/07/21 15:49:27 [INFO] Configuration file location: /Users/hudaalsobhi/OneDrive/Blockchain-workspace/IBMM-workspace/blockchain/blockchain_credentials/austr
alia_education_project/fabric-samples/test-network/organizations/peerOrganizations/org2.example.com/fabric-ca-client-config.yaml
2023/07/21 15:49:27 [INFO] TLS Enabled
2023/07/21 15:49:27 [INFO] TLS Enabled
```

Figure 5.9: Bringing up the network and creating a channel (4th figure of 12)

```
Password: org2adminpw
Generating the peer0 msp
+ fabric-ca-client enroll -u https://peer0:peer0pw@localhost:8054 --caname ca-org2 -M /Users/hudaalsobhi/OneDrive/Blockchain-workspace/IBMM-workspace/blockchai
n/blockchain_credentials/australia_education_project/fabric-samples/test-network/organizations/peerOrganizations/org2.example.com/peers/peer0.org2.example.com/
msp --csr.hosts peer0.org2.example.com --tls.certfiles /Users/hudaalsobhi/OneDrive/Blockchain-workspace/IBMM-workspace/blockchain/blockchain_credentials/austra
lia_education_project/fabric-samples/test-network/organizations/fabric-ca/org2/ca-cert.pem
2023/07/21 15:49:27 [INFO] TLS Enabled
2023/07/21 15:49:27 [INFO] generating key: &{A:ecdsa S:256}
2023/07/21 15:49:27 [INFO] encoded CSR
2023/07/21 15:49:27 [INFO] Stored client certificate at /Users/hudaalsobhi/OneDrive/Blockchain-workspace/IBMM-workspace/blockchain/blockchain_credentials/austr
alia_education_project/fabric-samples/test-network/organizations/peerOrganizations/org2.example.com/peers/peer0.org2.example.com/msp/signcerts/cert.pem
2023/07/21 15:49:27 [INFO] Stored root CA certificate at /Users/hudaalsobhi/OneDrive/Blockchain-workspace/IBMM-workspace/blockchain/blockchain_credentials/aust
ralia_education_project/fabric-samples/test-network/organizations/peerOrganizations/org2.example.com/peers/peer0.org2.example.com/msp/cacerts/localhost-8054-ca
-org2.pem
2023/07/21 15:49:27 [INFO] Stored Issuer public key at /Users/hudaalsobhi/OneDrive/Blockchain-workspace/IBMM-workspace/blockchain/blockchain_credentials/austra
lia_education_project/fabric-samples/test-network/organizations/peerOrganizations/org2.example.com/peers/peer0.org2.example.com/msp/IssuerPublicKey
2023/07/21 15:49:27 [INFO] Stored Issuer revocation public key at /Users/hudaalsobhi/OneDrive/Blockchain-workspace/IBMM-workspace/blockchain/blockchain_credent
ials/australia_education_project/fabric-samples/test-network/organizations/peerOrganizations/org2.example.com/peers/peer0.org2.example.com/msp/IssuerRevocation
PublicKey
Generating the peer0-tls certificates
+ fabric-ca-client enroll -u https://peer0:peer0pw@localhost:8054 --caname ca-org2 -M /Users/hudaalsobhi/OneDrive/Blockchain-workspace/IBMM-workspace/blockchai
n/blockchain_credentials/australia_education_project/fabric-samples/test-network/organizations/peerOrganizations/org2.example.com/peers/peer0.org2.example.com/
tls --enrollment.profile tls --csr.hosts peer0.org2.example.com --csr.hosts localhost --tls.certfiles /Users/hudaalsobhi/OneDrive/Blockchain-workspace/IBMM-wor
kspace/blockchain/blockchain_credentials/australia_education_project/fabric-samples/test-network/organizations/fabric-ca/org2/ca-cert.pem
2023/07/21 15:49:27 [INFO] TLS Enabled
2023/07/21 15:49:27 [INFO] generating key: &{A:ecdsa S:256}
2023/07/21 15:49:27 [INFO] encoded CSR
2023/07/21 15:49:27 [INFO] Stored client certificate at /Users/hudaalsobhi/OneDrive/Blockchain-workspace/IBMM-workspace/blockchain/blockchain_credentials/austr
alia_education_project/fabric-samples/test-network/organizations/peerOrganizations/org2.example.com/peers/peer0.org2.example.com/tls/signcerts/cert.pem
2023/07/21 15:49:27 [INFO] Stored TLS root CA certificate at /Users/hudaalsobhi/OneDrive/Blockchain-workspace/IBMM-workspace/blockchain/blockchain_credentials/
australia_education_project/fabric-samples/test-network/organizations/peerOrganizations/org2.example.com/peers/peer0.org2.example.com/tls/tlscacerts/tls-localh
ost-8054-ca-org2.pem
2023/07/21 15:49:27 [INFO] Stored Issuer public key at /Users/hudaalsobhi/OneDrive/Blockchain-workspace/IBMM-workspace/blockchain/blockchain_credentials/austra
lia_education_project/fabric-samples/test-network/organizations/peerOrganizations/org2.example.com/peers/peer0.org2.example.com/tls/IssuerPublicKey
2023/07/21 15:49:27 [INFO] Stored Issuer revocation public key at /Users/hudaalsobhi/OneDrive/Blockchain-workspace/IBMM-workspace/blockchain/blockchain_credent
ials/australia_education_project/fabric-samples/test-network/organizations/peerOrganizations/org2.example.com/peers/peer0.org2.example.com/tls/IssuerRevocation
PublicKey
Generating the user msp
+ fabric-ca-client enroll -u https://user1:user1pw@localhost:8054 --caname ca-org2 -M /Users/hudaalsobhi/OneDrive/Blockchain-workspace/IBMM-workspace/blockchai
n/blockchain_credentials/australia_education_project/fabric-samples/test-network/organizations/peerOrganizations/org2.example.com/users/User1@org2.example.com/
msp --tls.certfiles /Users/hudaalsobhi/OneDrive/Blockchain-workspace/IBMM-workspace/blockchain/blockchain_credentials/australia_education_project/fabric-sample
s/test-network/organizations/fabric-ca/org2/ca-cert.pem
2023/07/21 15:49:27 [INFO] TLS Enabled
```

Figure 5.10: Bringing up the network and creating a channel (5th figure of 12)

- Enroll a new student in organizations 1 or 2: Figure 5.25 shows that the chaincode is being invoked successfully to initiate a new transfer to the ledger using the "AddStudent" function, containing personal data (student-name, student-email,

```
2023/07/21 15:49:27 [INFO] generating key: &{A:ecdsa S:256}
2023/07/21 15:49:27 [INFO] encoded CSR
2023/07/21 15:49:27 [INFO] Stored client certificate at /Users/hudaalsobhi/OneDrive/Blockchain-workspace/IBMM-workspace/blockchain/blockchain_credentials/austr
alia_education_project/fabric-samples/test-network/organizations/peerOrganizations/org2.example.com/users/User1@org2.example.com/msp/signcerts/cert.pem
2023/07/21 15:49:27 [INFO] Stored root CA certificate at /Users/hudaalsobhi/OneDrive/Blockchain-workspace/IBMM-workspace/blockchain/blockchain_credentials/aust
ralia_education_project/fabric-samples/test-network/organizations/peerOrganizations/org2.example.com/users/User1@org2.example.com/msp/cacerts/localhost-8054-ca
-org2.pem
2023/07/21 15:49:27 [INFO] Stored Issuer public key at /Users/hudaalsobhi/OneDrive/Blockchain-workspace/IBMM-workspace/blockchain/blockchain_credentials/austra
lia_education_project/fabric-samples/test-network/organizations/peerOrganizations/org2.example.com/users/User1@org2.example.com/msp/IssuerPublicKey
2023/07/21 15:49:27 [INFO] Stored Issuer revocation public key at /Users/hudaalsobhi/OneDrive/Blockchain-workspace/IBMM-workspace/blockchain/blockchain_credent
ials/australia_education_project/fabric-samples/test-network/organizations/peerOrganizations/org2.example.com/users/User1@org2.example.com/msp/IssuerRevocation
PublicKey
Generating the org admin msp
+ fabric-ca-client enroll -u https://org2admin:org2adminpw@localhost:8054 --caname ca-org2 -M /Users/hudaalsobhi/OneDrive/Blockchain-workspace/IBMM-workspace/b
lockchain/blockchain_credentials/australia_education_project/fabric-samples/test-network/organizations/peerOrganizations/org2.example.com/users/Admin@org2.exam
ple.com/msp --tls.certfiles /Users/hudaalsobhi/OneDrive/Blockchain-workspace/IBMM-workspace/blockchain/blockchain_credentials/australia_education_project/fabri
c-samples/test-network/organizations/fabric-ca/org2/ca-cert.pem
2023/07/21 15:49:27 [INFO] TLS Enabled
2023/07/21 15:49:27 [INFO] generating key: &{A:ecdsa S:256}
2023/07/21 15:49:27 [INFO] encoded CSR
2023/07/21 15:49:27 [INFO] Stored client certificate at /Users/hudaalsobhi/OneDrive/Blockchain-workspace/IBMM-workspace/blockchain/blockchain_credentials/austr
alia_education_project/fabric-samples/test-network/organizations/peerOrganizations/org2.example.com/users/Admin@org2.example.com/msp/signcerts/cert.pem
2023/07/21 15:49:27 [INFO] Stored root CA certificate at /Users/hudaalsobhi/OneDrive/Blockchain-workspace/IBMM-workspace/blockchain/blockchain_credentials/aust
ralia_education_project/fabric-samples/test-network/organizations/peerOrganizations/org2.example.com/users/Admin@org2.example.com/msp/cacerts/localhost-8054-ca
-org2.pem
2023/07/21 15:49:27 [INFO] Stored Issuer public key at /Users/hudaalsobhi/OneDrive/Blockchain-workspace/IBMM-workspace/blockchain/blockchain_credentials/austra
lia_education_project/fabric-samples/test-network/organizations/peerOrganizations/org2.example.com/users/Admin@org2.example.com/msp/IssuerPublicKey
2023/07/21 15:49:27 [INFO] Stored Issuer revocation public key at /Users/hudaalsobhi/OneDrive/Blockchain-workspace/IBMM-workspace/blockchain/blockchain_credent
ials/australia_education_project/fabric-samples/test-network/organizations/peerOrganizations/org2.example.com/users/Admin@org2.example.com/msp/IssuerRevocation
PublicKey
Creating Orderer Org Identities
Enrolling the CA admin
+ fabric-ca-client enroll -u https://admin:adminpw@localhost:9054 --caname ca-orderer --tls.certfiles /Users/hudaalsobhi/OneDrive/Blockchain-workspace/IBMM-wor
kspace/blockchain/blockchain_credentials/australia_education_project/fabric-samples/test-network/organizations/fabric-ca/ordererOrg/ca-cert.pem
2023/07/21 15:49:28 [INFO] Created a default configuration file at /Users/hudaalsobhi/OneDrive/Blockchain-workspace/IBMM-workspace/blockchain/blockchain_creden
tials/australia_education_project/fabric-samples/test-network/organizations/ordererOrganizations/example.com/fabric-ca-client-config.yaml
2023/07/21 15:49:28 [INFO] TLS Enabled
2023/07/21 15:49:28 [INFO] generating key: &{A:ecdsa S:256}
2023/07/21 15:49:28 [INFO] encoded CSR
2023/07/21 15:49:28 [INFO] Stored client certificate at /Users/hudaalsobhi/OneDrive/Blockchain-workspace/IBMM-workspace/blockchain/blockchain_credentials/austr
alia_education_project/fabric-samples/test-network/organizations/ordererOrganizations/example.com/msp/signcerts/cert.pem
2023/07/21 15:49:28 [INFO] Stored root CA certificate at /Users/hudaalsobhi/OneDrive/Blockchain-workspace/IBMM-workspace/blockchain/blockchain_credentials/aust
ralia_education_project/fabric-samples/test-network/organizations/ordererOrganizations/example.com/msp/cacerts/localhost-9054-ca-orderer.pem
```

Figure 5.11: Bringing up the network and creating a channel (6th figure of 12)

```
2023/07/21 15:49:28 [INFO] Stored Issuer public key at /Users/hudaalsobhi/OneDrive/Blockchain-workspace/IBMM-workspace/blockchain/blockchain_credentials/austra
lia_education_project/fabric-samples/test-network/organizations/ordererOrganizations/example.com/msp/IssuerPublicKey
2023/07/21 15:49:28 [INFO] Stored Issuer revocation public key at /Users/hudaalsobhi/OneDrive/Blockchain-workspace/IBMM-workspace/blockchain/blockchain_credent
ials/australia_education_project/fabric-samples/test-network/organizations/ordererOrganizations/example.com/msp/IssuerRevocationPublicKey
Registering orderer
+ fabric-ca-client register --caname ca-orderer --id.name orderer --id.secret ordererpw --id.type orderer --tls.certfiles /Users/hudaalsobhi/OneDrive/Blockchai
n-workspace/IBMM-workspace/blockchain/blockchain_credentials/australia_education_project/fabric-samples/test-network/organizations/fabric-ca/ordererOrg/ca-cert
.pem
2023/07/21 15:49:28 [INFO] Configuration file location: /Users/hudaalsobhi/OneDrive/Blockchain-workspace/IBMM-workspace/blockchain/blockchain_credentials/austr
alia_education_project/fabric-samples/test-network/organizations/ordererOrganizations/example.com/fabric-ca-client-config.yaml
2023/07/21 15:49:28 [INFO] TLS Enabled
2023/07/21 15:49:28 [INFO] TLS Enabled
Password: ordererpw
Registering the orderer admin
+ fabric-ca-client register --caname ca-orderer --id.name ordererAdmin --id.secret ordererAdminpw --id.type admin --tls.certfiles /Users/hudaalsobhi/OneDrive/B
lockchain-workspace/IBMM-workspace/blockchain/blockchain_credentials/australia_education_project/fabric-samples/test-network/organizations/fabric-ca/ordererOrg
/ca-cert.pem
2023/07/21 15:49:28 [INFO] Configuration file location: /Users/hudaalsobhi/OneDrive/Blockchain-workspace/IBMM-workspace/blockchain/blockchain_credentials/austr
alia_education_project/fabric-samples/test-network/organizations/ordererOrganizations/example.com/fabric-ca-client-config.yaml
2023/07/21 15:49:28 [INFO] TLS Enabled
2023/07/21 15:49:28 [INFO] TLS Enabled
Password: ordererAdminpw
Generating the orderer msp
+ fabric-ca-client enroll -u https://orderer:ordererpw@localhost:9054 --caname ca-orderer -M /Users/hudaalsobhi/OneDrive/Blockchain-workspace/IBMM-workspace/bl
ockchain/blockchain_credentials/australia_education_project/fabric-samples/test-network/organizations/ordererOrganizations/example.com/orderers/orderer.example
.com/msp --csr.hosts orderer.example.com --csr.hosts localhost --tls.certfiles /Users/hudaalsobhi/OneDrive/Blockchain-workspace/IBMM-workspace/blockchain/block
chain_credentials/australia_education_project/fabric-samples/test-network/organizations/fabric-ca/ordererOrg/ca-cert.pem
2023/07/21 15:49:28 [INFO] TLS Enabled
2023/07/21 15:49:28 [INFO] generating key: &{A:ecdsa S:256}
2023/07/21 15:49:28 [INFO] encoded CSR
2023/07/21 15:49:28 [INFO] Stored client certificate at /Users/hudaalsobhi/OneDrive/Blockchain-workspace/IBMM-workspace/blockchain/blockchain_credentials/austr
alia_education_project/fabric-samples/test-network/organizations/ordererOrganizations/example.com/orderers/orderer.example.com/msp/signcerts/cert.pem
2023/07/21 15:49:28 [INFO] Stored root CA certificate at /Users/hudaalsobhi/OneDrive/Blockchain-workspace/IBMM-workspace/blockchain/blockchain_credentials/aust
ralia_education_project/fabric-samples/test-network/organizations/ordererOrganizations/example.com/orderers/orderer.example.com/msp/cacerts/localhost-9054-ca-o
rderer.pem
2023/07/21 15:49:28 [INFO] Stored Issuer public key at /Users/hudaalsobhi/OneDrive/Blockchain-workspace/IBMM-workspace/blockchain/blockchain_credentials/austra
lia_education_project/fabric-samples/test-network/organizations/ordererOrganizations/example.com/orderers/orderer.example.com/msp/IssuerPublicKey
2023/07/21 15:49:28 [INFO] Stored Issuer revocation public key at /Users/hudaalsobhi/OneDrive/Blockchain-workspace/IBMM-workspace/blockchain/blockchain_credent
ials/australia_education_project/fabric-samples/test-network/organizations/ordererOrganizations/example.com/orderers/orderer.example.com/msp/IssuerRevocationPu
blicKey
Generating the orderer-tls certificates
+ fabric-ca-client enroll -u https://orderer:ordererpw@localhost:9054 --caname ca-orderer -M /Users/hudaalsobhi/OneDrive/Blockchain-workspace/IBMM-workspace/bl
ockchain/blockchain_credentials/australia_education_project/fabric-samples/test-network/organizations/ordererOrganizations/example.com/orderers/orderer.example
```

Figure 5.12: Bringing up the network and creating a channel (7th figure of 12)

student-address, student-contact number, student-date of birth). In addition, the smart contract generates a unique ID/pseudonym for this student using the SHA-256 algorithm.

```
.com/tls --enrollment.profile tls --csr.hosts orderer.example.com --csr.hosts localhost --tls.certfiles /Users/hudaalsobhi/OneDrive/Blockchain-workspace/IBMM-w
orkspace/blockchain/blockchain_credentials/australia_education_project/fabric-samples/test-network/organizations/fabric-ca/ordererOrg/ca-cert.pem
2023/07/21 15:49:28 [INFO] TLS Enabled
2023/07/21 15:49:28 [INFO] generating key: &{A:ecdsa S:256}
2023/07/21 15:49:28 [INFO] encoded CSR
2023/07/21 15:49:28 [INFO] Stored client certificate at /Users/hudaalsobhi/OneDrive/Blockchain-workspace/IBMM-workspace/blockchain/blockchain_credentials/austr
alia_education_project/fabric-samples/test-network/organizations/ordererOrganizations/example.com/orderers/orderer.example.com/tls/signcerts/cert.pem
2023/07/21 15:49:28 [INFO] Stored TLS root CA certificate at /Users/hudaalsobhi/OneDrive/Blockchain-workspace/IBMM-workspace/blockchain/blockchain_credentials/
australia_education_project/fabric-samples/test-network/organizations/ordererOrganizations/example.com/orderers/orderer.example.com/tls/tlscacerts/tls-localhos
t-9054-ca-orderer.pem
2023/07/21 15:49:28 [INFO] Stored Issuer public key at /Users/hudaalsobhi/OneDrive/Blockchain-workspace/IBMM-workspace/blockchain/blockchain_credentials/austra
lia_education_project/fabric-samples/test-network/organizations/ordererOrganizations/example.com/orderers/orderer.example.com/tls/IssuerPublicKey
2023/07/21 15:49:28 [INFO] Stored Issuer revocation public key at /Users/hudaalsobhi/OneDrive/Blockchain-workspace/IBMM-workspace/blockchain/blockchain_credent
ials/australia_education_project/fabric-samples/test-network/organizations/ordererOrganizations/example.com/orderers/orderer.example.com/tls/IssuerRevocationPu
blicKey
Generating the admin msp
+ fabric-ca-client enroll -u https://ordererAdmin:ordererAdminpw@localhost:9054 --caname ca-orderer -M /Users/hudaalsobhi/OneDrive/Blockchain-workspace/IBMM-wo
rkspace/blockchain/blockchain_credentials/australia_education_project/fabric-samples/test-network/organizations/ordererOrganizations/example.com/users/Admin@ex
ample.com/msp --tls.certfiles /Users/hudaalsobhi/OneDrive/Blockchain-workspace/IBMM-workspace/blockchain/blockchain_credentials/australia_education_project/fab
ric-samples/test-network/organizations/fabric-ca/ordererOrg/ca-cert.pem
2023/07/21 15:49:29 [INFO] TLS Enabled
2023/07/21 15:49:29 [INFO] generating key: &{A:ecdsa S:256}
2023/07/21 15:49:29 [INFO] encoded CSR
2023/07/21 15:49:29 [INFO] Stored client certificate at /Users/hudaalsobhi/OneDrive/Blockchain-workspace/IBMM-workspace/blockchain/blockchain_credentials/austr
alia_education_project/fabric-samples/test-network/organizations/ordererOrganizations/example.com/users/Admin@example.com/msp/signcerts/cert.pem
2023/07/21 15:49:29 [INFO] Stored root CA certificate at /Users/hudaalsobhi/OneDrive/Blockchain-workspace/IBMM-workspace/blockchain/blockchain_credentials/aust
ralia_education_project/fabric-samples/test-network/organizations/ordererOrganizations/example.com/users/Admin@example.com/msp/cacerts/localhost-9054-ca-ordere
r.pem
2023/07/21 15:49:29 [INFO] Stored Issuer public key at /Users/hudaalsobhi/OneDrive/Blockchain-workspace/IBMM-workspace/blockchain/blockchain_credentials/austra
lia_education_project/fabric-samples/test-network/organizations/ordererOrganizations/example.com/users/Admin@example.com/msp/IssuerPublicKey
2023/07/21 15:49:29 [INFO] Stored Issuer revocation public key at /Users/hudaalsobhi/OneDrive/Blockchain-workspace/IBMM-workspace/blockchain/blockchain_credent
ials/australia_education_project/fabric-samples/test-network/organizations/ordererOrganizations/example.com/users/Admin@example.com/msp/IssuerRevocationPublicK
ey
Generating CCP files for Org1 and Org2
Docker Compose is now in the Docker CLI, try `docker compose up`

Creating volume "compose_orderer.example.com" with default driver
Creating volume "compose_peer0.org1.example.com" with default driver
Creating volume "compose_peer0.org2.example.com" with default driver
WARNING: Found orphan containers (ca_org2, ca_org1, ca_orderer) for this project. If you removed or renamed this service in your compose file, you can run this
 command with the --remove-orphans flag to clean it up.
Creating couchdb1            ... done
Creating orderer.example.com    ... done
```

Figure 5.13: Bringing up the network and creating a channel (8th figure of 12)

```
Creating orderer.example.com    ... done
Creating couchdb0               ... done
Creating peer0.org2.example.com ... done
Creating peer0.org1.example.com ... done
Creating cli                    ... done
CONTAINER ID   IMAGE                               COMMAND                  CREATED          STATUS                  PORTS
                                                                                            NAMES
e19f03841afd   hyperledger/fabric-tools:latest     "/bin/bash"              3 seconds ago    Up Less than a second
                                                                                            cli
bc71e8a4d73d   hyperledger/fabric-peer:latest      "peer node start"        11 seconds ago   Up 2 seconds            0.0.0.0:7051->7051/tcp, :::7051->7051/tcp,
 0.0.0.0:9444->9444/tcp, :::9444->9444/tcp                                                  peer0.org1.example.com
897289ca709f   hyperledger/fabric-peer:latest      "peer node start"        13 seconds ago   Up 6 seconds            0.0.0.0:9051->9051/tcp, :::9051->9051/tcp,
 7051/tcp, 0.0.0.0:9445->9445/tcp, :::9445->9445/tcp                                        peer0.org2.example.com
8df0723eda51   hyperledger/fabric-orderer:latest   "orderer"                17 seconds ago   Up 4 seconds            0.0.0.0:7050->7050/tcp, :::7050->7050/tcp,
 0.0.0.0:7053->7053/tcp, :::7053->7053/tcp, 0.0.0.0:9443->9443/tcp, :::9443->9443/tcp   orderer.example.com
f12a5358a37f   couchdb:3.1.1                       "tini -- /docker-ent…"   17 seconds ago   Up 12 seconds           4369/tcp, 9100/tcp, 0.0.0.0:7984->5984/tcp
, :::7984->5984/tcp                                                                         couchdb1
1b9814dd1c76   couchdb:3.1.1                       "tini -- /docker-ent…"   17 seconds ago   Up 11 seconds           4369/tcp, 9100/tcp, 0.0.0.0:5984->5984/tcp
, :::5984->5984/tcp                                                                         couchdb0
56c2615ecea5   hyperledger/fabric-ca:latest        "sh -c 'fabric-ca-se…"   34 seconds ago   Up 23 seconds           0.0.0.0:7054->7054/tcp, :::7054->7054/tcp,
 0.0.0.0:17054->17054/tcp, :::17054->17054/tcp                                              ca_org1
7df07c0e19e9   hyperledger/fabric-ca:latest        "sh -c 'fabric-ca-se…"   34 seconds ago   Up 26 seconds           0.0.0.0:8054->8054/tcp, :::8054->8054/tcp,
 7054/tcp, 0.0.0.0:18054->18054/tcp, :::18054->18054/tcp                                    ca_org2
d63309613fcc   hyperledger/fabric-ca:latest        "sh -c 'fabric-ca-se…"   34 seconds ago   Up 24 seconds           0.0.0.0:9054->9054/tcp, :::9054->9054/tcp,
 7054/tcp, 0.0.0.0:19054->19054/tcp, :::19054->19054/tcp                                    ca_orderer
Using docker and docker-compose
Generating channel genesis block 'mychannel.block'
/Users/hudaalsobhi/OneDrive/Blockchain-workspace/IBMM-workspace/blockchain/blockchain_credentials/australia_education_project/fabric-samples/test-network/../bi
n/configtxgen
+ configtxgen -profile TwoOrgsApplicationGenesis -outputBlock ./channel-artifacts/mychannel.block -channelID mychannel
2023-07-21 15:49:47.475 AEST [common.tools.configtxgen] main -> INFO 001 Loading configuration
2023-07-21 15:49:47.488 AEST [common.tools.configtxgen.localconfig] completeInitialization -> INFO 002 orderer type: etcdraft
2023-07-21 15:49:47.488 AEST [common.tools.configtxgen.localconfig] completeInitialization -> INFO 003 Orderer.EtcdRaft.Options unset, setting to tick_interval
:"500ms" election_tick:10 heartbeat_tick:1 max_inflight_blocks:5 snapshot_interval_size:16777216
2023-07-21 15:49:47.488 AEST [common.tools.configtxgen.localconfig] Load -> INFO 004 Loaded configuration: /Users/hudaalsobhi/OneDrive/Blockchain-workspace/IBM
M-workspace/blockchain/blockchain_credentials/australia_education_project/fabric-samples/test-network/configtx/configtx.yaml
2023-07-21 15:49:47.493 AEST [common.tools.configtxgen] doOutputBlock -> INFO 005 Generating genesis block
2023-07-21 15:49:47.493 AEST [common.tools.configtxgen] doOutputBlock -> WARN 006 Genesis block does not contain a consortiums group definition.  This block ca
nnot be used for orderer bootstrap.
2023-07-21 15:49:47.494 AEST [common.tools.configtxgen] doOutputBlock -> INFO 007 Writing genesis block
+ res=0
Creating channel mychannel
Using organization 1
```

Figure 5.14: Bringing up the network and creating a channel (9th figure of 12)

- Add a new micro-credential to the new student's profile using their pseudonym: "c9436cd547d67e5914bcdf198c8b338c7fc8d8a004cc4b46b8cad2f6e0dd05d7": Figure 5.26 shows that the chaincode is being invoked successfully to initiate a new

```
+ osnadmin channel join --channelID mychannel --config-block ./channel-artifacts/mychannel.block -o localhost:7053 --ca-file /Users/hudaalsobhi/OneDrive/Blockc
hain-workspace/IBMM-workspace/blockchain/blockchain_credentials/australia_education_project/fabric-samples/test-network/organizations/ordererOrganizations/exam
ple.com/tlsca/tlsca.example.com-cert.pem --client-cert /Users/hudaalsobhi/OneDrive/Blockchain-workspace/IBMM-workspace/blockchain/blockchain_credentials/austra
lia_education_project/fabric-samples/test-network/organizations/ordererOrganizations/example.com/orderers/orderer.example.com/tls/server.crt --client-key /User
s/hudaalsobhi/OneDrive/Blockchain-workspace/IBMM-workspace/blockchain/blockchain_credentials/australia_education_project/fabric-samples/test-network/organizati
ons/ordererOrganizations/example.com/orderers/orderer.example.com/tls/server.key
+ res=0
Status: 201
{
        "name": "mychannel",
        "url": "/participation/v1/channels/mychannel",
        "consensusRelation": "consenter",
        "status": "active",
        "height": 1
}

Channel 'mychannel' created
Joining org1 peer to the channel...
Using organization 1
+ peer channel join -b ./channel-artifacts/mychannel.block
+ res=0
2023-07-21 15:49:53.840 AEST [channelCmd] InitCmdFactory -> INFO 001 Endorser and orderer connections initialized
2023-07-21 15:49:54.064 AEST [channelCmd] executeJoin -> INFO 002 Successfully submitted proposal to join channel
Joining org2 peer to the channel...
Using organization 2
+ peer channel join -b ./channel-artifacts/mychannel.block
+ res=0
2023-07-21 15:49:57.303 AEST [channelCmd] InitCmdFactory -> INFO 001 Endorser and orderer connections initialized
2023-07-21 15:49:57.977 AEST [channelCmd] executeJoin -> INFO 002 Successfully submitted proposal to join channel
Setting anchor peer for org1...
Using organization 1
Fetching channel config for channel mychannel
Using organization 1
Fetching the most recent configuration block for the channel
+ peer channel fetch config config_block.pb -o orderer.example.com:7050 --ordererTLSHostnameOverride orderer.example.com -c mychannel --tls --cafile /opt/gopat
h/src/github.com/hyperledger/fabric/peer/organizations/ordererOrganizations/example.com/tlsca/tlsca.example.com-cert.pem
2023-07-21 05:49:58.686 UTC 0001 INFO [channelCmd] InitCmdFactory -> Endorser and orderer connections initialized
2023-07-21 05:49:58.696 UTC 0002 INFO [cli.common] readBlock -> Received block: 0
2023-07-21 05:49:58.696 UTC 0003 INFO [channelCmd] fetch -> Retrieving last config block: 0
2023-07-21 05:49:58.701 UTC 0004 INFO [cli.common] readBlock -> Received block: 0
Decoding config block to JSON and isolating config to Org1MSPconfig.json
+ configtxlator proto_decode --input config_block.pb --type common.Block --output config_block.json
+ jq '.data.data[0].payload.data.config' config_block.json
```

Figure 5.15: Bringing up the network and creating a channel (10th figure of 12)

```
+ jq '.channel_group.groups.Application.groups.Org1MSP.values += {"AnchorPeers":{"mod_policy": "Admins","value":{"anchor_peers": [{"host": "peer0.org1.example.
com","port": 7051}]},"version": "0"}}' Org1MSPconfig.json
Generating anchor peer update transaction for Org1 on channel mychannel
+ configtxlator proto_encode --input Org1MSPconfig.json --type common.Config --output original_config.pb
+ configtxlator proto_encode --input Org1MSPmodified_config.json --type common.Config --output modified_config.pb
+ configtxlator compute_update --channel_id mychannel --original original_config.pb --updated modified_config.pb --output config_update.pb
+ configtxlator proto_decode --input config_update.pb --type common.ConfigUpdate --output config_update.json
+ jq .
++ cat config_update.json
+ echo '{"payload":{"header":{"channel_header":{"channel_id":"mychannel", "type":2}},"data":{"config_update":{' '"channel_id":' '"mychannel",' '"isolated_data"
:' '{},' '"read_set":' '{' '"groups":' '{' '"Application":' '{' '"groups":' '{' '"Org1MSP":' '{' '"groups":' '{},' '"mod_policy":' '"",' '"policies":' '{' '"Ad
mins":' '{' '"mod_policy":' '"",' '"policy":' null, '"version":' '"0"' '},' '"Endorsement":' '{' '"mod_policy":' '"",' '"policy":' null, '"version":' '"0"' '},
' '"Readers":' '{' '"mod_policy":' '"",' '"policy":' null, '"version":' '"0"' '},' '"Writers":' '{' '"mod_policy":' '"",' '"policy":' null, '"version":' '"0"'
'}' '},' '"values":' '{' '"MSP":' '{' '"mod_policy":' '"",' '"value":' null, '"version":' '"0"' '}' '},' '"version":' '"0"' '}' '},' '"mod_policy":' '"",' '"po
licies":' '{},' '"values":' '{},' '"version":' '"0"' '}' '},' '"mod_policy":' '"",' '"policies":' '{},' '"values":' '{},' '"version":' '"0"' '},' '"write_set":
' '{' '"groups":' '{' '"Application":' '{' '"groups":' '{' '"Org1MSP":' '{' '"groups":' '{},' '"mod_policy":' '"Admins"," '"policies":' '{' '"Admins":' '{' '"m
od_policy":' '"",' '"policy":' null, '"version":' '"0"' '},' '"Endorsement":' '{' '"mod_policy":' '"",' '"policy":' null, '"version":' '"0"' '},' '"Readers":'
'{' '"mod_policy":' '"",' '"policy":' null, '"version":' '"0"' '},' '"Writers":' '{' '"mod_policy":' '"",' '"policy":' null, '"version":' '"0"' '}' '},' '"valu
es":' '{' '"AnchorPeers":' '{' '"mod_policy":' '"Admins"," '"value":' '{' '"anchor_peers":' '[' '{' '"host":' '"peer0.org1.example.com"," '"port":' 7051 '}' ']
' '},' '"version":' '"0"' '},' '"MSP":' '{' '"mod_policy":' '"",' '"value":' null, '"version":' '"0"' '}' '},' '"version":' '"1"' '}' '},' '"mod_policy":' '"",
' '"policies":' '{},' '"values":' '{},' '"version":' '"0"' '}' '},' '"mod_policy":' '"",' '"policies":' '{},' '"values":' '{},' '"version":' '"0"' '}' '}}}}'
+ configtxlator proto_encode --input config_update_in_envelope.json --type common.Envelope --output Org1MSPanchors.tx
2023-07-21 05:49:59.076 UTC 0001 INFO [channelCmd] InitCmdFactory -> Endorser and orderer connections initialized
2023-07-21 05:49:59.095 UTC 0002 INFO [channelCmd] update -> Successfully submitted channel update
Anchor peer set for org 'Org1MSP' on channel 'mychannel'
Setting anchor peer for org2...
Using organization 2
Fetching channel config for channel mychannel
Using organization 2
Fetching the most recent configuration block for the channel
+ peer channel fetch config config_block.pb -o orderer.example.com:7050 --ordererTLSHostnameOverride orderer.example.com -c mychannel --tls --cafile /opt/gopat
h/src/github.com/hyperledger/fabric/peer/organizations/ordererOrganizations/example.com/tlsca/tlsca.example.com-cert.pem
2023-07-21 05:49:59.492 UTC 0001 INFO [channelCmd] InitCmdFactory -> Endorser and orderer connections initialized
2023-07-21 05:49:59.497 UTC 0002 INFO [cli.common] readBlock -> Received block: 1
2023-07-21 05:49:59.497 UTC 0003 INFO [channelCmd] fetch -> Retrieving last config block: 1
2023-07-21 05:49:59.499 UTC 0004 INFO [cli.common] readBlock -> Received block: 1
+ configtxlator proto_decode --input config_block.pb --type common.Block --output config_block.json
Decoding config block to JSON and isolating config to Org2MSPconfig.json
+ jq '.data.data[0].payload.data.config' config_block.json
+ jq '.channel_group.groups.Application.groups.Org2MSP.values += {"AnchorPeers":{"mod_policy": "Admins","value":{"anchor_peers": [{"host": "peer0.org2.example.
com","port": 9051}]},"version": "0"}}' Org2MSPconfig.json
Generating anchor peer update transaction for Org2 on channel mychannel
+ configtxlator proto_encode --input Org2MSPconfig.json --type common.Config --output original_config.pb
```

Figure 5.16: Bringing up the network and creating a channel (11th figure of 12)

transfer to the ledger using the "AddCredential" function, containing student-id, credential-id, credential-name, credential-subject, credential-date, credential-mark.

```
+ configtxlator proto_encode --input Org2MSPmodified_config.json --type common.Config --output modified_config.pb
+ configtxlator compute_update --channel_id mychannel --original original_config.pb --updated modified_config.pb --output config_update.pb
+ configtxlator proto_decode --input config_update.pb --type common.ConfigUpdate --output config_update.json
+ jq .
++ cat config_update.json
+ echo '{"payload":{"header":{"channel_header":{"channel_id":"mychannel", "type":2}},"data":{"config_update":{' '"channel_id":' '"mychannel",' '"isolated_data"
:' '{},' '"read_set":' '{' '"groups":' '{' '"Application":' '{' '"groups":' '{' '"Org2MSP":' '{' '"groups":' '{},' '"mod_policy":' '"",' '"policies":' '{' '"Ad
mins":' '{' '"mod_policy":' '"",' '"policy":' null, '"version":' '"0"' '},' '"Endorsement":' '{' '"mod_policy":' '"",' '"policy":' null, '"version":' '"0"' '},
' '"Readers":' '{' '"mod_policy":' '"",' '"policy":' null, '"version":' '"0"' '},' '"Writers":' '{' '"mod_policy":' '"",' '"policy":' null, '"version":' '"0"'
'}' '},' '"values":' '{' '"MSP":' '{' '"mod_policy":' '"",' '"value":' null, '"version":' '"0"' '}' '},' '"version":' '"0"' '}' '},' '"mod_policy":' '"",' '"po
licies":' '{},' '"values":' '{},' '"version":' '"0"' '}' '},' '"mod_policy":' '"",' '"policies":' '{},' '"values":' '{},' '"version":' '"0"' '},' '"write_set":
' '{' '"groups":' '{' '"Application":' '{' '"groups":' '{' '"Org2MSP":' '{' '"groups":' '{},' '"mod_policy":' '"Admins",' '"policies":' '{' '"Admins":' '{' '"m
od_policy":' '"",' '"policy":' null, '"version":' '"0"' '},' '"Endorsement":' '{' '"mod_policy":' '"",' '"policy":' null, '"version":' '"0"' '},' '"Readers":'
'{' '"mod_policy":' '"",' '"policy":' null, '"version":' '"0"' '},' '"Writers":' '{' '"mod_policy":' '"",' '"policy":' null, '"version":' '"0"' '}' '},' '"valu
es":' '{' '"AnchorPeers":' '{' '"mod_policy":' '"Admins",' '"value":' '{' '"anchor_peers":' '[' '{' '"host":' '"peer0.org2.example.com",' '"port":' 9051 '}' ']
' '},' '"version":' '"0"' '},' '"MSP":' '{' '"mod_policy":' '"",' '"value":' null, '"version":' '"0"' '}' '},' '"version":' '"1"' '}' '},' '"mod_policy":' '"",
' '"policies":' '{},' '"values":' '{},' '"version":' '"0"' '}' '},' '"mod_policy":' '"",' '"policies":' '{},' '"values":' '{},' '"version":' '"0"' '}' '}}}}'
+ configtxlator proto_encode --input config_update_in_envelope.json --type common.Envelope --output Org2MSPanchors.tx
2023-07-21 05:49:59.724 UTC 0001 INFO [channelCmd] InitCmdFactory -> Endorser and orderer connections initialized
2023-07-21 05:49:59.738 UTC 0002 INFO [channelCmd] update -> Successfully submitted channel update
Anchor peer set for org 'Org2MSP' on channel 'mychannel'
Channel 'mychannel' joined
```

Figure 5.17: Bringing up the network and creating a channel (12th figure of 12)

```
hudaalsobhi@192-168-1-164 ~/OneDrive/Blockchain-workspace/IBMM-workspace/blockchain/blockchain_credentials/australia_education_project/fabric-samples/test-netw
ork % docker ps -a

CONTAINER ID   IMAGE
                    COMMAND                   CREATED          STATUS          PORTS
                                                 NAMES
8959c09a71bd   dev-peer0.org1.example.com-basic_1.0-0ce3e2814328fc92a01ad92d5a10233351960f236c7707e05a99d9c10aad1d64-89fa74364414662ff28fd70de5ac448928f435431f
f5f1410af6d9680fe1549f   "docker-entrypoint.s…"   45 minutes ago   Up 44 minutes
                                                 dev-peer0.org1.example.com-basic_1.0-0ce3e2814328fc92a01ad92d5a10233351960f236c7707e05a99d9c10aad1d64
0ef217964241   dev-peer0.org2.example.com-basic_1.0-0ce3e2814328fc92a01ad92d5a10233351960f236c7707e05a99d9c10aad1d64-f531403d53ed24025239d51c5d8fdc50eac64603bd
7fd6c2fa189814274814c3   "docker-entrypoint.s…"   45 minutes ago   Up 44 minutes
                                                 dev-peer0.org2.example.com-basic_1.0-0ce3e2814328fc92a01ad92d5a10233351960f236c7707e05a99d9c10aad1d64
fd03e92ae12b   hyperledger/fabric-tools:latest
                    "/bin/bash"               46 minutes ago   Up 46 minutes
                                                 cli
aef2aa0c97d1   hyperledger/fabric-peer:latest
                    "peer node start"         47 minutes ago   Up 46 minutes   0.0.0.0:7051->7051/tcp, :::7051->7051/tcp, 0.0.0.0:9444->9444/tcp, :::9444->
9444/tcp                                         peer0.org1.example.com
dfc4140ed4dd   hyperledger/fabric-peer:latest
                    "peer node start"         47 minutes ago   Up 46 minutes   0.0.0.0:9051->9051/tcp, :::9051->9051/tcp, 7051/tcp, 0.0.0.0:9445->9445/tcp,
 :::9445->9445/tcp                               peer0.org2.example.com
74b95c35a28b   hyperledger/fabric-orderer:latest
                    "orderer"                 47 minutes ago   Up 46 minutes   0.0.0.0:7050->7050/tcp, :::7050->7050/tcp, 0.0.0.0:7053->7053/tcp, :::7053->
7053/tcp, 0.0.0.0:9443->9443/tcp, :::9443->9443/tcp   orderer.example.com
ea2168e2bc7b   couchdb:3.1.1
                    "tini -- /docker-ent…"    47 minutes ago   Up 47 minutes   4369/tcp, 9100/tcp, 0.0.0.0:5984->5984/tcp, :::5984->5984/tcp
                                                 couchdb0
92920a16f986   couchdb:3.1.1
                    "tini -- /docker-ent…"    47 minutes ago   Up 47 minutes   4369/tcp, 9100/tcp, 0.0.0.0:7984->5984/tcp, :::7984->5984/tcp
                                                 couchdb1
cf76a47889f8   hyperledger/fabric-ca:latest
                    "sh -c 'fabric-ca-se…"    47 minutes ago   Up 47 minutes   0.0.0.0:7054->7054/tcp, :::7054->7054/tcp, 0.0.0.0:17054->17054/tcp, :::1705
4->17054/tcp                                     ca_org1
48da6ade92f1   hyperledger/fabric-ca:latest
                    "sh -c 'fabric-ca-se…"    47 minutes ago   Up 47 minutes   0.0.0.0:8054->8054/tcp, :::8054->8054/tcp, 7054/tcp, 0.0.0.0:18054->18054/tc
p, :::18054->18054/tcp                           ca_org2
845443fbdf90   hyperledger/fabric-ca:latest
                    "sh -c 'fabric-ca-se…"    47 minutes ago   Up 47 minutes   0.0.0.0:9054->9054/tcp, :::9054->9054/tcp, 7054/tcp, 0.0.0.0:19054->19054/tc
p, :::19054->19054/tcp                           ca_orderer
```

Figure 5.18: Docker containers

- Add a new action plan to the student's profile using their pseudonym: "c9436cd547d67e5914bcdf198c8b338c7fc8d8a004cc4b46b8cad2f6e0dd05d7": Figure 5.27 shows that the chaincode is being invoked successfully to initiate a new transfer to the ledger using the "AddActionPlan" function, containing student-id, plan-id, plan-duration, plan-subject, plan-cost, institution-name.

- Read the profile of the new student who has registered previously using the "ReadStudentWithID" function, containing their pseudonym: "c9436cd547d67e5914bcdf198c8b338c7fc8d8a004cc4b46b8cad2f6e0dd05d7": Figure 5.28 displays the student's profile including personal information, micro-credentials, and action plans.

```
hudaalsobhi@192-168-1-164 ~/OneDrive/Blockchain-workspace/IBMM-workspace/blockchain/blockchain_credentials/australia_education_project/fabric-samples/test-netw
ork % ./network.sh deployCC -ccn basic -ccp ../credit-transfer-basic/chaincode-typescript -ccl typescript

Using docker and docker-compose
deploying chaincode on channel 'mychannel'
executing with the following
- CHANNEL_NAME: mychannel
- CC_NAME: basic
- CC_SRC_PATH: ../credit-transfer-basic/chaincode-typescript
- CC_SRC_LANGUAGE: typescript
- CC_VERSION: 1.0
- CC_SEQUENCE: 1
- CC_END_POLICY: NA
- CC_COLL_CONFIG: NA
- CC_INIT_FCN: NA
- DELAY: 3
- MAX_RETRY: 5
- VERBOSE: false
Compiling TypeScript code into JavaScript...
~/OneDrive/Blockchain-workspace/IBMM-workspace/blockchain/blockchain_credentials/australia_education_project/fabric-samples/credit-transfer-basic/chaincode-typ
escript ~/OneDrive/Blockchain-workspace/IBMM-workspace/blockchain/blockchain_credentials/australia_education_project/fabric-samples/test-network
npm WARN asset-transfer-basic@1.0.0 No repository field.

up to date in 1.169s

> asset-transfer-basic@1.0.0 build /Users/hudaalsobhi/Library/CloudStorage/OneDrive-Personal/Blockchain-workspace/IBMM-workspace/blockchain/blockchain_credenti
als/australia_education_project/fabric-samples/credit-transfer-basic/chaincode-typescript
> tsc


    Update available 5.5.1 → 9.8.1
    Run npm i -g npm to update


~/OneDrive/Blockchain-workspace/IBMM-workspace/blockchain/blockchain_credentials/australia_education_project/fabric-samples/test-network
Finished compiling TypeScript code into JavaScript
+ peer lifecycle chaincode package basic.tar.gz --path ../credit-transfer-basic/chaincode-typescript --lang node --label basic_1.0
+ res=0
Chaincode is packaged
```

Figure 5.19: Deploying the chaincode (1st figure of 4)

```
Installing chaincode on peer0.org1...
Using organization 1
+ peer lifecycle chaincode install basic.tar.gz
+ res=0
2023-07-24 13:32:33.509 AEST [cli.lifecycle.chaincode] submitInstallProposal -> INFO 001 Installed remotely: response:<status:200 payload:"\nJbasic_1.0:af32277
95a66b828e7eafa47cbd12376dc2da371a1971b27fe58bddfa773a698\022\tbasic_1.0" >
2023-07-24 13:32:33.510 AEST [cli.lifecycle.chaincode] submitInstallProposal -> INFO 002 Chaincode code package identifier: basic_1.0:af3227795a66b828e7eafa47c
bd12376dc2da371a1971b27fe58bddfa773a698
Chaincode is installed on peer0.org1
Install chaincode on peer0.org2...
Using organization 2
+ peer lifecycle chaincode install basic.tar.gz
+ res=0
2023-07-24 13:32:53.361 AEST [cli.lifecycle.chaincode] submitInstallProposal -> INFO 001 Installed remotely: response:<status:200 payload:"\nJbasic_1.0:af32277
95a66b828e7eafa47cbd12376dc2da371a1971b27fe58bddfa773a698\022\tbasic_1.0" >
2023-07-24 13:32:53.361 AEST [cli.lifecycle.chaincode] submitInstallProposal -> INFO 002 Chaincode code package identifier: basic_1.0:af3227795a66b828e7eafa47c
bd12376dc2da371a1971b27fe58bddfa773a698
Chaincode is installed on peer0.org2
Using organization 1
+ peer lifecycle chaincode queryinstalled
+ res=0
Installed chaincodes on peer:
Package ID: basic_1.0:af3227795a66b828e7eafa47cbd12376dc2da371a1971b27fe58bddfa773a698, Label: basic_1.0
Query installed successful on peer0.org1 on channel
Using organization 1
+ peer lifecycle chaincode approveformyorg -o localhost:7050 --ordererTLSHostnameOverride orderer.example.com --tls --cafile /Users/hudaalsobhi/OneDrive/Blockc
hain-workspace/IBMM-workspace/blockchain/blockchain_credentials/australia_education_project/fabric-samples/test-network/organizations/ordererOrganizations/examp
bd12376dc2da371a1971b27fe58bddfa773a698 --sequence 1
+ res=0
2023-07-24 13:32:55.852 AEST [chaincodeCmd] ClientWait -> INFO 001 txid [fb78d097d0329a2c3098d8a2ff03f86286a5fc92d80245642e643eef20e863e0] committed with statu
s (VALID) at localhost:7051
Chaincode definition approved on peer0.org1 on channel 'mychannel'
Using organization 1
Checking the commit readiness of the chaincode definition on peer0.org1 on channel 'mychannel'...
Attempting to check the commit readiness of the chaincode definition on peer0.org1, Retry after 3 seconds.
+ peer lifecycle chaincode checkcommitreadiness --channelID mychannel --name basic --version 1.0 --sequence 1 --output json
+ res=0
{
        "approvals": {
                "Org1MSP": true,
                "Org2MSP": false
        }
}
```

Figure 5.20: Deploying the chaincode (2nd figure of 4)

Furthermore, the chaincode container logs for Container ID: 8959c09a71bd can be displayed, which shows all the processes conducted on the chaincode as shown in Figure 5.29.

```
Checking the commit readiness of the chaincode definition successful on peer0.org1 on channel 'mychannel'
Using organization 2
Checking the commit readiness of the chaincode definition on peer0.org2 on channel 'mychannel'...
Attempting to check the commit readiness of the chaincode definition on peer0.org2, Retry after 3 seconds.
+ peer lifecycle chaincode checkcommitreadiness --channelID mychannel --name basic --version 1.0 --sequence 1 --output json
+ res=0
{
        "approvals": {
                "Org1MSP": true,
                "Org2MSP": false
        }
}
Checking the commit readiness of the chaincode definition successful on peer0.org2 on channel 'mychannel'
Using organization 2
+ peer lifecycle chaincode approveformyorg -o localhost:7050 --ordererTLSHostnameOverride orderer.example.com --tls --cafile /Users/hudaalsobhi/OneDrive/Blockc
hain-workspace/IBMM-workspace/blockchain/blockchain_credentials/australia_education_project/fabric-samples/test-network/organizations/ordererOrganizations/exam
ple.com/tlsca/tlsca.example.com-cert.pem --channelID mychannel --name basic --version 1.0 --package-id basic_1.0:af3227795a66b828e7eafa47cbd12376dc2da371a1971b
27fe58bddfa773a698 --sequence 1
+ res=0
2023-07-24 13:33:04.502 AEST [chaincodeCmd] ClientWait -> INFO 001 txid [e9f14ae72a2ed04ae062fa55fe6f17cc7fb7c704334122653f99f5bb3417cf44] committed with statu
s (VALID) at localhost:9051
Chaincode definition approved on peer0.org2 on channel 'mychannel'
Using organization 1
Checking the commit readiness of the chaincode definition on peer0.org1 on channel 'mychannel'...
Attempting to check the commit readiness of the chaincode definition on peer0.org1, Retry after 3 seconds.
+ peer lifecycle chaincode checkcommitreadiness --channelID mychannel --name basic --version 1.0 --sequence 1 --output json
+ res=0
{
        "approvals": {
                "Org1MSP": true,
                "Org2MSP": true
        }
}
Checking the commit readiness of the chaincode definition successful on peer0.org1 on channel 'mychannel'
Using organization 2
Checking the commit readiness of the chaincode definition on peer0.org2 on channel 'mychannel'...
Attempting to check the commit readiness of the chaincode definition on peer0.org2, Retry after 3 seconds.
+ peer lifecycle chaincode checkcommitreadiness --channelID mychannel --name basic --version 1.0 --sequence 1 --output json
+ res=0
{
        "approvals": {
                "Org1MSP": true,
                "Org2MSP": true
        }
}
```

Figure 5.21: Deploying the chaincode (3rd figure of 4)

```
        }
}
Checking the commit readiness of the chaincode definition successful on peer0.org2 on channel 'mychannel'
Using organization 1
Using organization 2
+ peer lifecycle chaincode commit -o localhost:7050 --ordererTLSHostnameOverride orderer.example.com --tls --cafile /Users/hudaalsobhi/OneDrive/Blockchain-work
space/IBMM-workspace/blockchain/blockchain_credentials/australia_education_project/fabric-samples/test-network/organizations/ordererOrganizations/example.com/t
lsca/tlsca.example.com-cert.pem --channelID mychannel --name basic --peerAddresses localhost:7051 --tlsRootCertFiles /Users/hudaalsobhi/OneDrive/Blockchain-wor
kspace/IBMM-workspace/blockchain/blockchain_credentials/australia_education_project/fabric-samples/test-network/organizations/peerOrganizations/org1.example.co
m/tlsca/tlsca.org1.example.com-cert.pem --peerAddresses localhost:9051 --tlsRootCertFiles /Users/hudaalsobhi/OneDrive/Blockchain-workspace/IBMM-workspace/block
chain/blockchain_credentials/australia_education_project/fabric-samples/test-network/organizations/peerOrganizations/org2.example.com/tlsca/tlsca.org2.example.
com-cert.pem --version 1.0 --sequence 1
+ res=0
2023-07-24 13:33:12.963 AEST [chaincodeCmd] ClientWait -> INFO 001 txid [a84a6000522a2c9a9f687b069bdcad58174187d035e790a816ec51c5784647d8] committed with statu
s (VALID) at localhost:7051
2023-07-24 13:33:12.966 AEST [chaincodeCmd] ClientWait -> INFO 002 txid [a84a6000522a2c9a9f687b069bdcad58174187d035e790a816ec51c5784647d8] committed with statu
s (VALID) at localhost:9051
Chaincode definition committed on channel 'mychannel'
Using organization 1
Querying chaincode definition on peer0.org1 on channel 'mychannel'...
Attempting to Query committed status on peer0.org1, Retry after 3 seconds.
+ peer lifecycle chaincode querycommitted --channelID mychannel --name basic
+ res=0
Committed chaincode definition for chaincode 'basic' on channel 'mychannel':
Version: 1.0, Sequence: 1, Endorsement Plugin: escc, Validation Plugin: vscc, Approvals: [Org1MSP: true, Org2MSP: true]
Query chaincode definition successful on peer0.org1 on channel 'mychannel'
Using organization 2
Querying chaincode definition on peer0.org2 on channel 'mychannel'...
Attempting to Query committed status on peer0.org2, Retry after 3 seconds.
+ peer lifecycle chaincode querycommitted --channelID mychannel --name basic
+ res=0
Committed chaincode definition for chaincode 'basic' on channel 'mychannel':
Version: 1.0, Sequence: 1, Endorsement Plugin: escc, Validation Plugin: vscc, Approvals: [Org1MSP: true, Org2MSP: true]
Query chaincode definition successful on peer0.org2 on channel 'mychannel'
Chaincode initialization is not required
```

Figure 5.22: Deploying the chaincode (4th figure of 4)

```
hudaalsobhi@192-168-1-164 ~/OneDrive/Blockchain-workspace/IBMM-workspace/blockchain/blockchain_credentials/australia_education_project/fabric-samples/test-netw
ork % peer chaincode invoke -o localhost:7050 --ordererTLSHostnameOverride orderer.example.com --tls --cafile "${PWD}/organizations/ordererOrganizations/exampl
e.com/orderers/orderer.example.com/msp/tlscacerts/tlsca.example.com-cert.pem" -C mychannel -n basic --peerAddresses localhost:7051 --tlsRootCertFiles "${PWD}/o
rganizations/peerOrganizations/org1.example.com/peers/peer0.org1.example.com/tls/ca.crt" --peerAddresses localhost:9051 --tlsRootCertFiles "${PWD}/organization
s/peerOrganizations/org2.example.com/peers/peer0.org2.example.com/tls/ca.crt" -c '{"function":"InitLedger","Args":[]}'
2023-07-24 13:34:07.282 AEST [chaincodeCmd] chaincodeInvokeOrQuery -> INFO 001 Chaincode invoke successful. result: status:200
```

Figure 5.23: Invoking the chaincode

Figure 5.24: Getting all the students

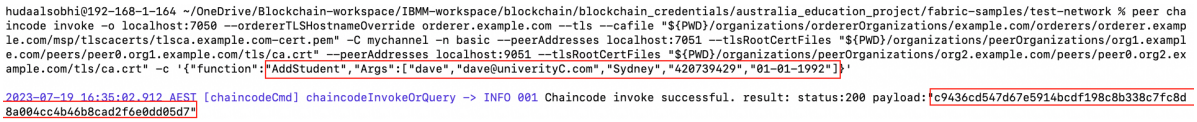

Figure 5.25: Enrolling a new student

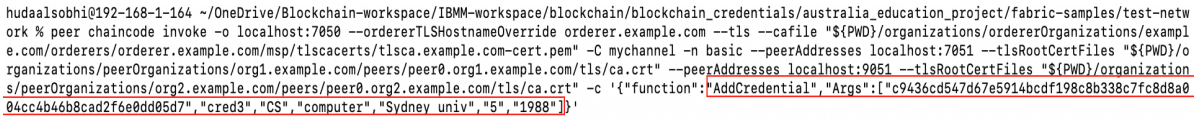

Figure 5.26: Adding a new micro-credential

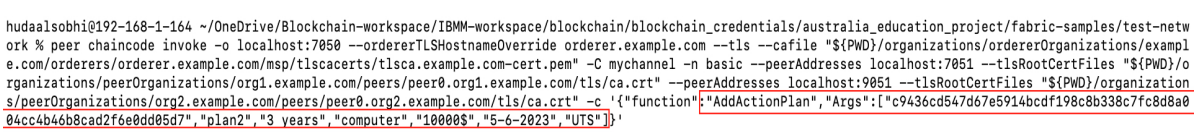

Figure 5.27: Adding a new action plan

```
hudaalsobhi@192-168-1-164 ~/OneDrive/Blockchain-workspace/IBMM-workspace/blockchain/blockchain_credentials/australia_education_project/fabric-samples/test-network % peer cha
incode query -C mychannel -n basic -c '{"Args":["ReadStudentWithID","c9436cd547d67e5914bcdf198c8b338c7fc8d8a004cc4b46b8cad2f6e0dd05d7"]}' | jq
{
  "ActionPlan": [
    {
      "Institution_Name": "UTS",
      "Plan_Cost": "10000$",
      "Plan_Date": "5-6-2023",
      "Plan_Duration": "3 years",
      "Plan_ID": "plan2",
      "Plan_Subject": "computer"
    }
  ],
  "Credential": [
    {
      "Credential_Date": "1988",
      "Credential_ID": "cred3",
      "Credential_Mark": "5",
      "Credential_Name": "CS",
      "Credential_Subject": "computer",
      "Institution_Name": "Sydney univ"
    }
  ],
  "Student_Address": "Sydney",
  "Student_Contact_Number": "420739429",
  "Student_Date_of_Birth": "01-01-1992",
  "Student_Email": "d003426af50ba32551c5b1586ce99f0be5d134c019f3f35f919cc398eef58d96",
  "Student_ID": "c9436cd547d67e5914bcdf198c8b338c7fc8d8a004cc4b46b8cad2f6e0dd05d7",
  "Student_Name": "61ea0803f8853523b777d414ace3130cd4d3f92de2cd7ff8695c337d79c2eeee",
  "docType": "student"
}
```

Figure 5.28: Reading a student's profile using their ID

```
hudaalsobhi@192-168-1-164 ~/OneDrive/Blockchain-workspace/IBMM-workspace/blockchain/blockchain_credentials/australia_education_project/fabric-samples/test-network % docker logs 8959c09a71bd
2023-07-19T06:29:34.126Z info [c-api:lib/handler.js]                    [mychannel-604e68e6] Calling chaincode Invoke() succeeded. Sending COMPLETED message back to peer
The student ID is c9436cd547d67e5914bcdf198c8b338c7fc8d8a004cc4b46b8cad2f6e0dd05d7
student list in ledger
new student data getting into ledger {
  Student_ID: 'c9436cd547d67e5914bcdf198c8b338c7fc8d8a004cc4b46b8cad2f6e0dd05d7',
  Student_Name: '61ea0803f8853523b777d414ace3130cd4d3f92de2cd7ff8695c337d79c2eeee',
  Student_Email: 'd003426af50ba32551c5b1586ce99f0be5d134c019f3f35f919cc398eef58d96',
  Student_Address: 'Sydney',
  Student_Contact_Number: '420739429',
  Student_Date_of_Birth: '01-01-1992',
  Credential: [],
  ActionPlan: [],
  docType: 'student'
}
2023-07-19T06:35:02.929Z info [c-api:lib/handler.js]                    [mychannel-557bba3e] Calling chaincode Invoke() succeeded. Sending COMPLETED message back to peer
student data {"ActionPlan":[],"Credential":[],"Student_Address":"Sydney","Student_Contact_Number":"420739429","Student_Date_of_Birth":"01-01-1992","Student_Email":"d003426af50ba32551c5b1586ce99f0be5d134c019f3f35f919cc398eef58d96","Studen
t_ID":"c9436cd547d67e5914bcdf198c8b338c7fc8d8a004cc4b46b8cad2f6e0dd05d7","Student_Name":"61ea0803f8853523b777d414ace3130cd4d3f92de2cd7ff8695c337d79c2eeee","docType":"student"}
cred data object {
  Credential_ID: 'cred3',
  Credential_Name: 'CS',
  Credential_Subject: 'computer',
  Credential_Date: '1988',
  Credential_Mark: '5',
  Institution_Name: 'Sydney univ'
}
{
  ActionPlan: [],
  Credential: [],
  Student_Address: 'Sydney',
  Student_Contact_Number: '420739429',
  Student_Date_of_Birth: '01-01-1992',
  Student_Email: 'd003426af50ba32551c5b1586ce99f0be5d134c019f3f35f919cc398eef58d96',
  Student_ID: 'c9436cd547d67e5914bcdf198c8b338c7fc8d8a004cc4b46b8cad2f6e0dd05d7',
  Student_Name: '61ea0803f8853523b777d414ace3130cd4d3f92de2cd7ff8695c337d79c2eeee',
  docType: 'student'
}
2023-07-19T06:43:35.149Z info [c-api:lib/handler.js]                    [mychannel-cd6e6e4c] Calling chaincode Invoke() succeeded. Sending COMPLETED message back to peer
student data {"ActionPlan":[],"Credential":[{"Credential_Date":"1988","Credential_ID":"cred3","Credential_Mark":"5","Credential_Name":"CS","Credential_Subject":"computer","Institution_Name":"Sydney univ"}],"Student_Address":"Sydney","Stu
dent_Contact_Number":"420739429","Student_Date_of_Birth":"01-01-1992","Student_Email":"d003426af50ba32551c5b1586ce99f0be5d134c019f3f35f919cc398eef58d96","Student_ID":"c9436cd547d67e5914bcdf198c8b338c7fc8d8a004cc4b46b8cad2f6e0dd05d7","Stu
dent_Name":"61ea0803f8853523b777d414ace3130cd4d3f92de2cd7ff8695c337d79c2eeee","docType":"student"}
Action plan data object {
  Plan_ID: 'plan2',
  Plan_Duration: '3 years',
  Plan_Subject: 'computer',
  Plan_Cost: '10000$',
  Plan_Date: '5-6-2023',
  Institution_Name: 'UTS'
}
{
  ActionPlan: [],
  Credential: [
    {
      Credential_Date: '1988',
      Credential_ID: 'cred3',
      Credential_Mark: '5',
      Credential_Name: 'CS',
      Credential_Subject: 'computer',
      Institution_Name: 'Sydney univ'
    }
  ],
  Student_Address: 'Sydney',
  Student_Contact_Number: '420739429',
  Student_Date_of_Birth: '01-01-1992',
  Student_Email: 'd003426af50ba32551c5b1586ce99f0be5d134c019f3f35f919cc398eef58d96',
  Student_ID: 'c9436cd547d67e5914bcdf198c8b338c7fc8d8a004cc4b46b8cad2f6e0dd05d7',
  Student_Name: '61ea0803f8853523b777d414ace3130cd4d3f92de2cd7ff8695c337d79c2eeee',
  docType: 'student'
```

Figure 5.29: The chaincode container logs

- Get all HEIs that are already registered on the blockchain ledger using the "GetAllInstitustions" function: Figure 5.30 shows the information of three HEIs that are currently stored on the blockchain.
- Enroll a new HEI in organizations 1 or 2: Figure 5.31 shows that the chaincode is being invoked successfully to initiate a new transfer to the ledger using the

```
hudaalsobhi@192-168-1-164 ~/OneDrive/Blockchain-workspace/IBMM-workspace/blockchain/blockchain_credentials/australia_education_project/fabric-samples/test-netw
ork % peer chaincode query -C mychannel -n basic -c '{"Args":["GetAllInstitustions"]}' |  jq
[
  {
    "Institustion_Address": "sydney, AUS",
    "Institustion_Contact_Number": "0411705491",
    "Institustion_Email": "admin@universityB.com",
    "Institustion_ID": "2254809110",
    "Institustion_Name": "University B",
    "docType": "institution"
  },
  {
    "Institustion_Address": "queensLand, AUS",
    "Institustion_Contact_Number": "0456709781",
    "Institustion_Email": "admin@universityA.com",
    "Institustion_ID": "6530091124",
    "Institustion_Name": "University A",
    "docType": "institution"
  },
  {
    "Institustion_Address": "Melbourn, AUS",
    "Institustion_Contact_Number": "0433911000",
    "Institustion_Email": "admin@universityC.com",
    "Institustion_ID": "7722103821",
    "Institustion_Name": "University C",
    "docType": "institution"
  }
]
```

First institution

Second institution

Third institution

Figure 5.30: Getting all the higher education institutions (HEIs)

"AddInstitustion" function, containing (institution-id, institution-name, institution-email, institution-address, institution-contact number).

```
hudaalsobhi@192-168-1-164 ~/OneDrive/Blockchain-workspace/IBMM-workspace/blockchain/blockchain_credentials/australia_education_project/fabric-samples/test-netw
ork % peer chaincode invoke -o localhost:7050 --ordererTLSHostnameOverride orderer.example.com --tls --cafile "${PWD}/organizations/ordererOrganizations/exampl
e.com/orderers/orderer.example.com/msp/tlscacerts/tlsca.example.com-cert.pem" -C mychannel -n basic --peerAddresses localhost:7051 --tlsRootCertFiles "${PWD}/o
rganizations/peerOrganizations/org1.example.com/peers/peer0.org1.example.com/tls/ca.crt" --peerAddresses localhost:9051 --tlsRootCertFiles "${PWD}/organization
s/peerOrganizations/org2.example.com/peers/peer0.org2.example.com/tls/ca.crt" -c '{"function":"AddInstitustion","Args":["875614428","uts","uts@edu.au","goerge
street","0456 87432"]}'

2023-07-20 17:32:01.216 AEST [chaincodeCmd] chaincodeInvokeOrQuery -> INFO 001 Chaincode invoke successful. result: status:200
```

Figure 5.31: Enrolling a new HEI

All data stored on the Couch database that has been transferred to the blockchain ledger can be displayed, as shown in Figure 5.32.

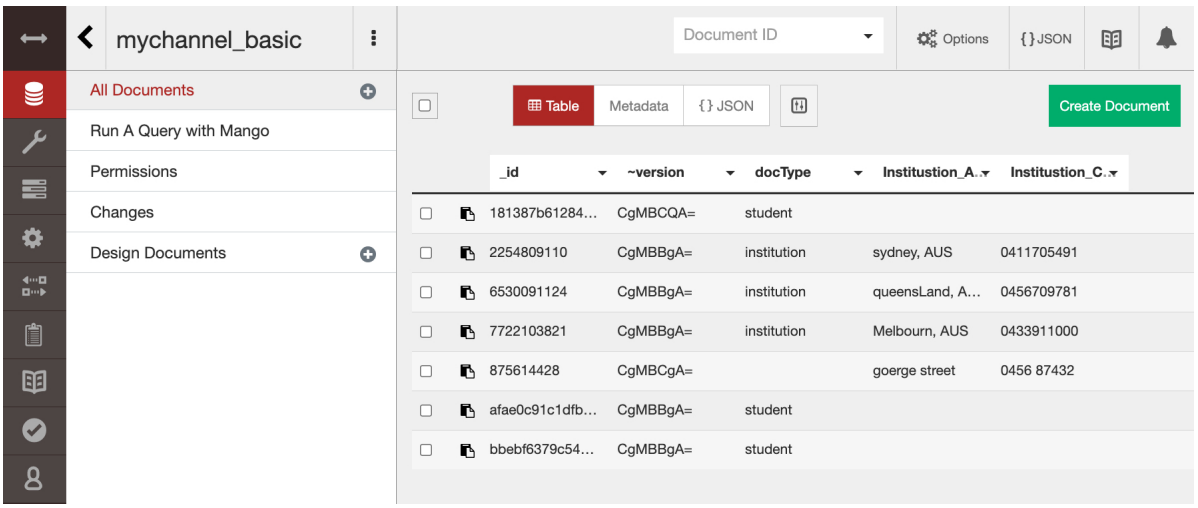

Figure 5.32: The database content

Figure 5.33 shows the information that is stored in the database on the student that was added recently (see Figure 5.25).

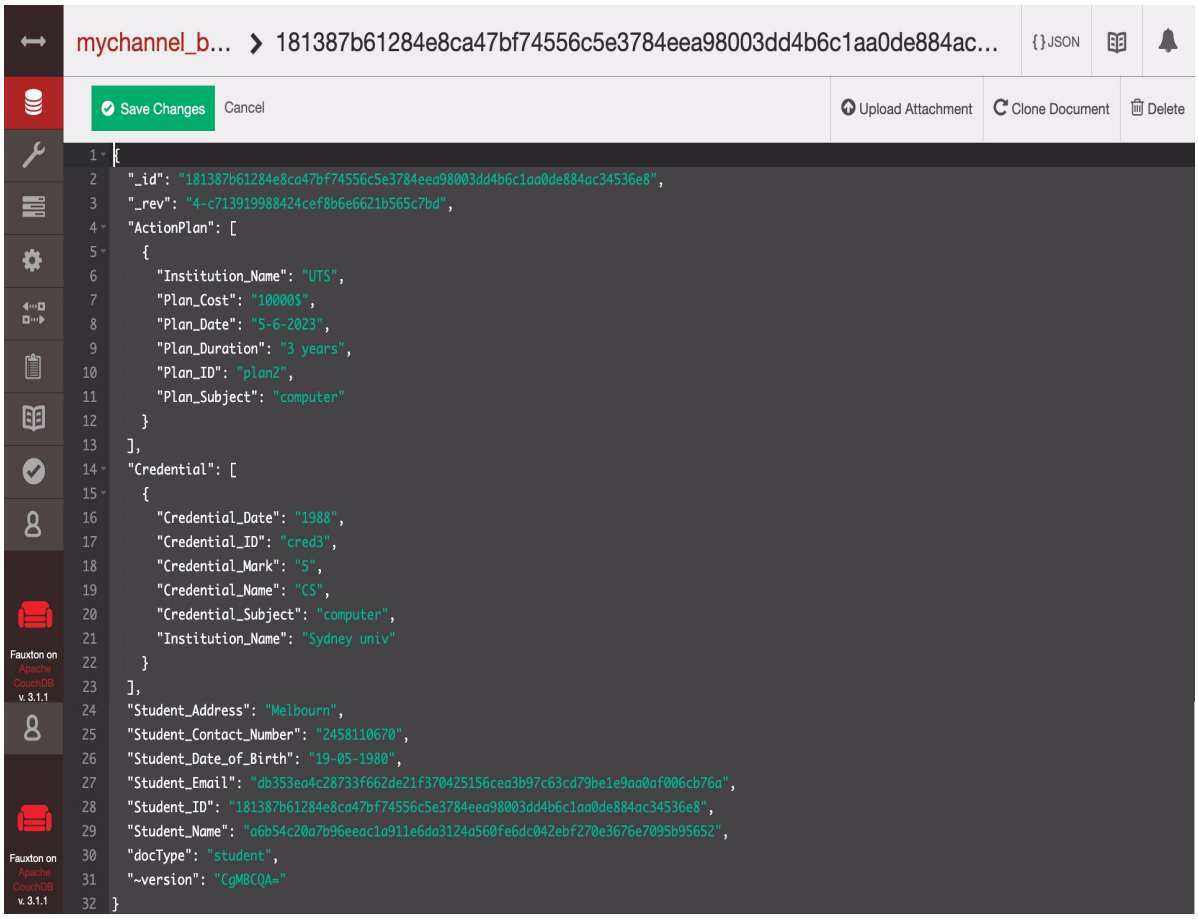

Figure 5.33: A student record on the database

Figure 5.34 shows the information that is stored in the database on the institution that was added recently (see Figure 5.31).

5.6.2 Validation process for the privacy-preserving technique

The following steps are utilized to validate the privacy-preserving technique that is used to address RQ2:

1. We select a sample of 100 students' identities from the "Higher Education Students Survey" dataset that is collected and described in Chapter 6 in Section 6.4, we use the students' email addresses and the students' names are extracted from their email addresses. The dataset can be found in the following link: `https://`

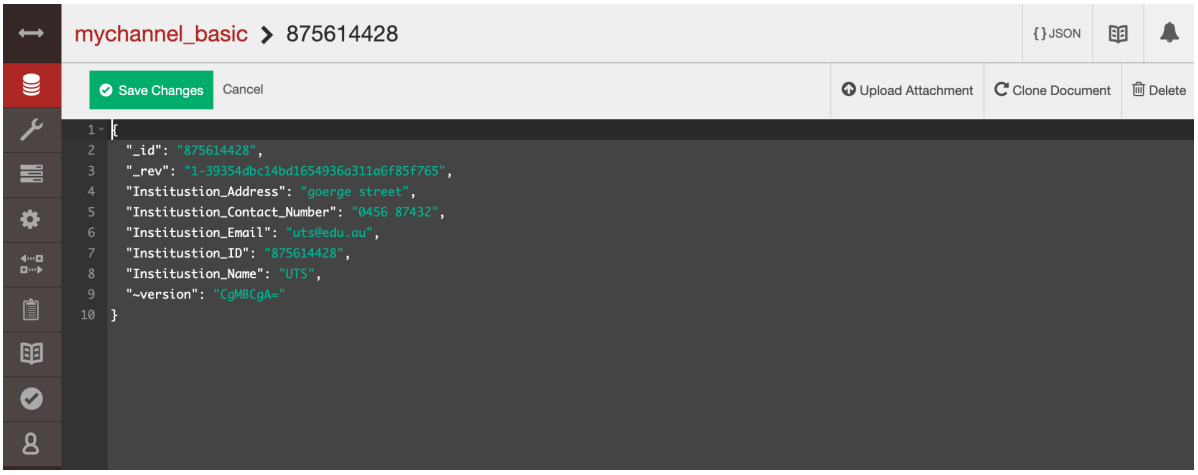

Figure 5.34: A higher education institution record on the database

studentutsedu-my.sharepoint.com/:f:/r/personal/hada_alsobhi_student_uts_edu_au/Documents/Datasets?csf=1&web=1&e=RhEsj7.

2. The hash function is applied to each student's identity to generate a pseudonym. We examined the effectiveness of the one-way hash function (SHA-256) by ensuring that no two different inputs produce identical hash values.

3. We use every pseudonym to access and view the student's profile. We also validate the algorithm's accuracy by evaluating whether the student's real identity is revealed when viewing their profile.

We interact with the chaincode using specific commands through the CLI, outlined as follows:

- When a new student is registered using the "AddStudent" function, the smart contract for the hash function is called to generate a pseudonym (unique ID) for the student as shown in Figure 5.25. First, the SHA-256 algorithm is applied to the student's name and email address separately to anonymize them. Then, these two hash values are combined, and again the hash algorithm is applied to the combined output to get a pseudonym. Figure 5.35 illustrates the registration of a new student and anonymizing their name and email address to generate a pseudonym.

- When a HEI tries to access a student's profile using their pseudonym, they can view the student's profile with anonymous data, so they can not identify this student, as shown in Figure 5.28. Figure 5.36 shows another student's profile when it is

```
hudaalsobhi@192-168-1-164 ~/OneDrive/Blockchain-workspace/IBMM-workspace/blockchain/blockchain_credentials/australia_education_project/fabric-samp
les/test-network % peer chaincode invoke -o localhost:7050 --ordererTLSHostnameOverride orderer.example.com --tls --cafile "${PWD}/organizations/o
rdererOrganizations/example.com/orderers/orderer.example.com/msp/tlscacerts/tlsca.example.com-cert.pem" -C mychannel -n basic --peerAddresses loca
lhost:7051 --tlsRootCertFiles "${PWD}/organizations/peerOrganizations/org1.example.com/peers/peer0.org1.example.com/tls/ca.crt" --peerAddresses lo
calhost:9051 --tlsRootCertFiles "${PWD}/organizations/peerOrganizations/org2.example.com/peers/peer0.org2.example.com/tls/ca.crt" -c '{"function":
"AddStudent","Args":["Amal","amal@univerityA.com","Melbourn","2458110670","19-05-1980"]}'

2023-07-24 13:36:20.000 AEST [chaincodeCmd] chaincodeInvokeOrQuery -> INFO 001 Chaincode invoke successful. result: status:200 payload:"314c3e7995
fdc4787b137ecb2d7932f21528a1af82f5546c699e6748a30387ce"
```

Figure 5.35: Enrol a new student

accessed using the student pseudonym that was generated in the previous step using the "ReadStudentWithID" function. HEIs can read all the data on students except their identities (name and email address) because these are presented anonymously.

```
hudaalsobhi@192-168-1-164 ~/OneDrive/Blockchain-workspace/IBMM-workspace/blockchain/blockchain_credentials/australia_education_project/fabric-samp
les/test-network % peer chaincode query -C mychannel -n basic -c '{"Args":["ReadStudentWithID","314c3e7995fdc4787b137ecb2d7932f21528a1af82f5546c69
9e6748a30387ce"]}' | jq

{
  "ActionPlan": [],
  "Credential": [],
  "Student_Address": "Melbourn",
  "Student_Contact_Number": "2458110670",
  "Student_Date_of_Birth": "19-05-1980",
  "Student_Email": "21bd10918a612ed131d6f0fd000776a9eaaabca69f1f93f28d307be8db7fe3c7",
  "Student_ID": "314c3e7995fdc4787b137ecb2d7932f21528a1af82f5546c699e6748a30387ce",
  "Student_Name": "47c5173c5568dc3c74d801dd43ca07b786df5f0c90e4442bca64a449bf730ed2",
  "docType": "student"
}
```

Figure 5.36: Accessing a student's profile

	Student_Email	Student_Name	Student_Psuedonym
2	sowel.mahmood@uts.edu.au	Sowel	a9fbe9852adc4b4c6ef1edae3fce5cea1922d725d77e8cf706f39472aada4c55
3	wafamatara.alharbi@student.uts.edu.au	Wafa	e5db9e037a8d8ceacb7736c9d8e9b96e90bcf82784ceb621f856d39f7dcae735
4	suhair.alotaibi@student.uts.edu.au	Suhair	a346c167e4e8bb5555f388d5c202d6143eff6e78b2a033d81a39be2a05a21ddf
5	mwaheb.almadani@student.uts.edu.au	Mwaheb	a52a026060987f2c448e6b82f5f9376cf5fa9a26269fe05e8b9d6536b6944d9f
6	abeer.mirdad@student.uts.edu.au	Abeer	d91814c836615c5f879fa344328a80cdb34f3745fe1acc2fe67c95cb15c09f06
7	rania.alhazmi@student.uts.edu.au	Rania	34fbe83e19f8a397832892e15d31ea83bcb71f6af05b8eafba700872e9c3fc85
8	mohrah.s.alalyan@student.uts.edu.au	Mohrah	f71917b9b1fb2c1a923cc994634992ad65d12d4559c67a975de885a726c8b44f
9	tian.xia@student.uts.edu.au	Tian	18d781b88ec9ff6ddc1ec4c5274ba8c70d78b102840933f144756e531701191d
10	inam.alanazi@student.uts.edu.au	Inam	e24b2c3b947198b3d015ebb8a535a7069da3eacfd1f42712a33c21bec035f527
11	rayed.alakhtar@student.uts.edu.au	Rayed	8a21e9ee4d7037574ed67085077e70beeb1c6a499a0170096684b856e6b03059
12	enaam.alshuaibi@student.uts.edu.au	Enaam	ebce2812d6c854b88e2bf6a5318fc8fa4784ca388f966039c24ef12378c78c03
13	shuraia.khan@uts.edu.au	Shuraia	c7982b41da12b2e2a0ab525c386d1d04c0075e93111085ddf68323697a538fca
14	adel.khwaji@student.uts.edu.au	Adel	64cc51b3b277627eee3add8ea60a442a88dd070a2bdb6d02b8e6ab1ff6f06b39
15	asma.alkhalaf@student.uts.edu.au	Asma	6dadce3c98854fc0e06fb8368b429cf9b5d48b3ef984cba5ba8bdf8dbb02039a
16	ibraheemabdulhafizq.khan@student.uts.edu.au	Ibraheem	6f0464df46a43837a07ee6911e05475d797bd2ddf8b3c31cfac40cbf0acdad27
17	AlaaMohammedA.Jawa@student.uts.edu.au	Alaa	fdd350c0530f26bec36da68f98334ade8789e13ae78516fa6eba5ea827f8b8ec
18	Yeman.Fan@student.uts.edu.au	Yeman	1ca06b05190742b8d21f66c90608eb0623d3066b5cfc8dc59b7b2e1398ee37bb
19	kurt.mikolajczyk@uts.edu.au	Kurt	d2b338d788fb8e198ac067ddf5aa97e5763ab330cccde7f4c27e4dffc85d1906
20	ebtesamhussain.almansor@student.uts.edu.au	Ebtesam	7f2f20b65ce9f494aa55d7794ef9a87835c46210b9104b6863c49b50a8972987

Figure 5.37: Screenshot of a selection of students' pseudnyms

The second objective addresses the privacy preservation of student data on the IBMM platform. Anonymization was achieved using the hashing algorithm. To validate this

solution, we tested it many times on 100 students by calling the "AddStudent" and "ReadStudentWithID" functions to generate a unique pseudonym for every student and then read their profile using this generated pseudonym. Figure 5.37 shows a screenshot of the students' names and email addresses and their generated pseudonyms. This process ensures that each student has a unique pseudonym and every time HEIs access a student's profile, their real identity is not disclosed.

5.7 Conclusion

This chapter provided a thorough explanation of the architecture and functions of the IBMM framework and its three layers. The development of the Hyperledger Fabric blockchain on our local device (MacOS) was also described. In addition, this chapter discussed the privacy-preserving technique that was applied to ensure student anonymity. The hashing algorithm that was used as the proposed solution to the second research question was also explained in this chapter. Moreover, a prototype evaluation for the IBMM framework and the validation process for the privacy-preserving technique was provided in this chapter. The prototype evaluation process provided significant insights into the effectiveness of the proposed solution for managing and maintaining micro-credentials in higher education. Key findings from the evaluation highlighted the robustness of our blockchain-based platform in securely storing, sharing, managing, and verifying students' micro-credentials while ensuring the anonymity of their real identities, thereby enhancing trust and efficiency in the higher education ecosystem. The proposed solution not only allows students to securely manage their academic records but also streamlines the process for HEIs to access these credentials while preserving student privacy.
The next chapter discusses the proposed solution to address the third research question in this thesis which focuses on developing a recommender system.

CHAPTER 6

IBMM: Intelligent Recommender System to Provide Recommendations for Students' Academic Majors

6.1 Introduction

Selecting the right major is a significant decision for university students, especially for students who are new to a particular field, as they may lack the experience and knowledge to make an informed decision, and they may encounter different factors that can influence their decision. An inappropriate choice of a major or course can have far-reaching implications for students and universities, and negatively impact the students' career prospects [85]. Moreover, the choice of an inappropriate major can lead to a lack of interest, low academic performance, and difficulty finding a suitable job [16]. Hence, it is vitally important that students select an appropriate major to avoid wasting their valuable time, budget, and the resources of the university. The selection of an appropriate major can have a substantial impact on a student's future earnings and career aspirations. Moreover, selecting an appropriate major can ensure that students match their interests with their learning and ensure they engage in deeper learning in their chosen field [16].

Many university students require guidance to select an appropriate major during their studies, hence there is a need for a recommender system to help students make an

informed decision. As outlined in several research studies, an automated recommender system can play a crucial role in recommending the most appropriate major to students based on their academic credentials [16, 85]. By utilizing such a recommender system, students can ensure that they select a major that aligns with their micro-credentials, academic performance, skills, and preferences.

An overview of the proposed solution for the third research question on developing a recommender system that can help students identify a suitable major was presented in Chapter 4. Chapter 5 described the design of the IBMM framework and its functionality and addressed the second research question. This chapter will provide a comprehensive explanation of the proposed intelligent solution to address the third research question which involves the development of a recommender system.

This chapter explains the functionality of our proposed recommender system as a solution to the third research question, which involves recommending a suitable major for a student to complete a particular degree based on their micro-credentials and academic profiles. In the following sections, the process of utilizing intelligent methods to recommend the most appropriate major for a student is detailed.

The structure of this chapter is as follows: Section 6.2 presents the intelligent solution for providing learning recommendations. Section 6.3 provides insights into the details of the recommender system developed in this thesis, as well as the machine learning algorithms chosen for its implementation. Section 6.4 presents the validation process and the results of the proposed solution and details the dataset utilized during the implementation phase of our recommender system. Finally, Section 6.5 concludes this chapter.

6.2 Solution Overview to Provide Recommendations for Students' Majors

This section details how the third research question of this thesis is addressed, which involves resolving the challenge of recommending a suitable academic major for a student during their course of study in a university.
To solve the problem facing university students in selecting an appropriate major dur-

ing their studies, it is essential to provide them with the necessary guidance to make informed decisions about their academic majors.
As explained in Chapter 4, the solution to this challenge is to develop a recommender system using intelligent techniques to generate recommendations for the most suitable majors for students based on their academic information and micro-credentials, thus aiding students in selecting a major that aligns with their interests and career goals [17]. Consequently, if students request assistance in identifying a major for the purpose of completing a specific degree, our recommender system on the IBMM platform can help in recommending a suitable major that takes into account their verified micro-credentials and other academic qualifications [17].

As elucidated in Chapter 5, after the students' micro-credentials are validated and stored on the blockchain ledger, the next step in generating learning recommendations for academic majors can be initiated.
We introduce the intelligent solution employed to tackle the third research question, which is ***how can a recommendation for a major be generated so that the users can complete their degree?***
To enhance the effectiveness of the recommendations, we leverage the capabilities of artificial intelligence (AI) and machine learning (ML) techniques when developing the recommender system.

6.3 Working of the Recommender System

A recommender system (RS) is a tool that uses artificial intelligence techniques to assist users in making suitable choices by providing appropriate recommendations based on their preferences and information [19]. Recommender systems are used in the education sector and other sectors, such as health and tourism, etc., to address similar issues [16]. In the education sector, recommender systems can provide personalized services to learners by identifying their academic profiles, skills, experiences, etc. This can be particularly useful for university students as it helps them determine the most suitable major based on their micro-credentials, preferences, and educational information. A recommender system can help students make educated decisions regarding their future academic careers and improve their chances of success by selecting the most suitable major.

Our developed recommender system utilizes real data collected from university students to assist them in identifying the optimal major that matches their interests, skills, preferences, academic qualifications, and micro-credentials. Figure 6.1 shows how this recommender system generates appropriate majors for students. It operates as follows:

- Firstly, data is collected from university students.
- Secondly, the dataset is preprocessed and the relevant features are selected.
- Thirdly, the dataset is divided into a training set for training the selected machine-learning models and a testing set for testing the models and predicting majors.
- Fourthly, the performance of all models is evaluated, and the model that best predicts the most suitable major for the student is selected.

The problem of recommending the best majors for students is viewed as a multi-class classification problem. Multi-class classification is a classification problem involving more than two classes [8]. In this type of problem, each sample is assumed to be assigned to only one class label. In our case, several majors, such as computer science & information technology, engineering, law, and etc. can be treated as different classes. It may be helpful to approach this issue as a multi-class classification problem to recommend the most suitable majors for students.

We use classification models to classify the input data into one of the classes and we provide the algorithm with labeled data, for example, samples of students with their recommended majors. The algorithm can learn from these samples and the labeled data, and a model that can predict the most appropriate major for a given student based on their features can be built.
Various ML and AI algorithms are used for multi-class classification problems, and we select the best of these, namely XGBoost, LightGBM, random forest, and multilayer perceptron (MLP) to assign each student to one major. These algorithms support multi-class prediction, they are able to effectively handle either large or small datasets with multiple classes, and they provide accurate classification results.
The training and testing dataset includes information about the students' features and academic performance, including (a) their highest degree achieved, (b) their current major, (c) their previous major, (d) their expected future major, (e) their previous micro-credentials, and (f) their gender and age. This data is used as input to train and test the

models, then each model predicts an outcome related to every student's major. Including this data will help to ensure that the models are as accurate and relevant as possible by considering the many factors that can impact a student's educational and professional trajectory.

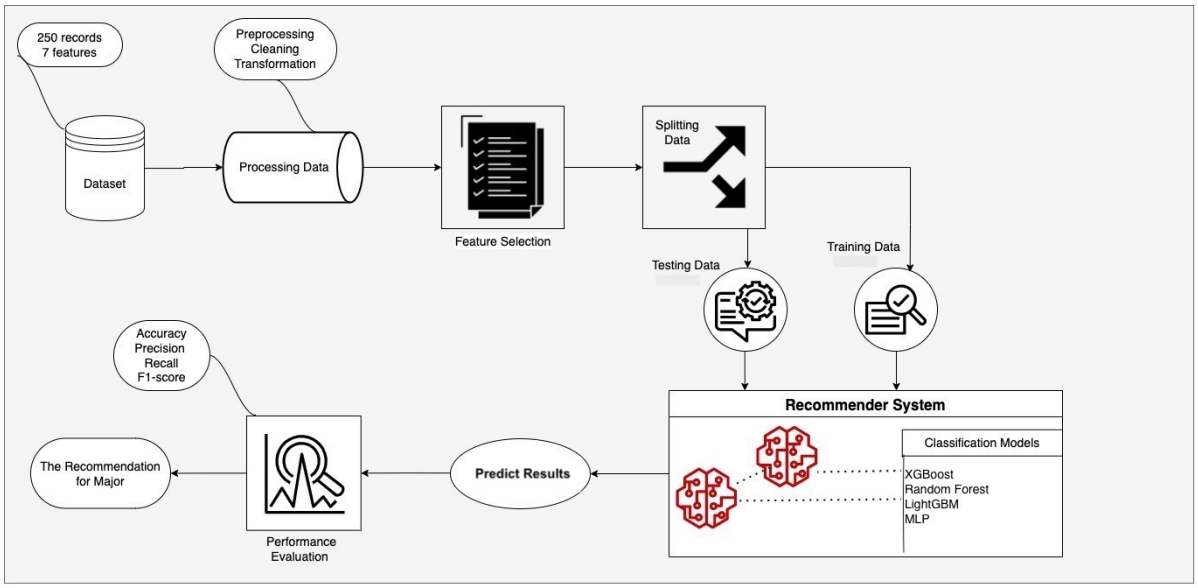

Figure 6.1: The architecture of the recommender system

6.3.1 Machine learning algorithms used in the development of the recommender system

The three supervised machine-learning models and the deep-learning model that are selected and utilized to address RQ3 are discussed as follows:

1. **Extreme Gradient Boosting (XGBoost):** XGBoost is one of the most popular machine learning algorithms based on decision trees and utilizes a process called boosting to enhance its performance [8]. Specifically, XGBoost executes gradient-boosted decision trees, which are specifically designed to be fast and efficient. XGBoost is considered a highly effective ensemble learning technique as it further builds on the gradient boosting framework to improve its speed and performance [8]. XGBoost classifier is a popular method for tackling multi-class classification problems and it has been shown to produce accurate and reliable results for a variety of multi-class classification tasks [8].

The XGBoost algorithm works by building decision trees in a sequential manner, where each new tree attempts to correct the errors made by the previous trees. The process starts with a single decision tree and then subsequent trees are added iteratively to the ensemble until the specified number of trees is reached or no further improvements can be made [8]. XGBoost uses the level-wise strategy and includes several additional features to enhance its performance, such as subsampling the training examples and features, tree pruning, and handling missing values [8].
In general, the XGBoost algorithm can be thought of as a weighted sum of decision trees, where each decision tree is trained on a training subset and is designed to correct the errors made by the previous trees [29]. The final prediction is obtained by summing the predictions of a sample in each tree, with each tree's contribution weighted by a coefficient that depends on the quality of the tree's predictions [29]. The prediction scores made by the XGBoost model are the weighted sum of the predictions made by each individual decision tree in the ensemble [29].
The formula for the final prediction is [29]:

$$y^{=} \sum_{k=1}^{K} f_k(x_i), f_k \in F \tag{6.1}$$

where K is the number of decision trees, f_k(x_i) is the predicted value or the function space of F, and F is the space of regression trees or CART. [29].
The overall goal of XGBoost is to perform accurate predictions on a range of machine learning problems by combining gradient boosting, regularisation methods, and decision tree ensemble learning [29].
We apply the XGBoost classifier model as the first method to classify students into their suitable majors. This machine learning (ML) model can predict appropriate majors based on student features. We use Python to apply the XGBoost classifier to our dataset and import the following libraries [29]:

- XGBoost is used to import all of the XGBoost library's functionality to access the full XGBoost functionality.
- Pandas is a powerful Python library that is used to manipulate, analyze, and work with structured data.
- Scikit-learn (sklearn) is a class used to split our dataset into training and testing sets.

- XGBClassifier represents a particular implementation of XGBoost that is designed to perform classification tasks.
- LabelEncoder is a class used to transform categorical values into numerical values.

The random_state parameter is set to ensure reproducibility. The performance of the XGBoost model is evaluated based on the accuracy metric. The code to implement the XGBoost classifier method to classify the students into major classes can be accessed via the following link: `https://github.com/hudaalsobhi/IBMM-code.git`.

2. **Random Forest (RF):** Random forest is a classifier composed of multiple decision tree models. It uses the concept of bagging ensemble learning, which involves combining multiple classifiers to solve complex problems and enhance the accuracy of predictions. As the number of decision trees increases, the random forest model becomes more robust [83].
   The algorithm produces a class which is the mode of the individual decision trees. This is achieved by constructing several decision trees on various subsets of the dataset and taking the average of their outputs [83]. The random forest algorithm utilizes three key hyperparameters, namely node size, number of trees, and number of sampled features. These parameters aim to improve model performance and predictive ability [83]. The random forest algorithm operates in the following manner: first, it randomly chooses samples from a provided dataset or training set; second, it constructs decision trees for each training data using the algorithm; and third, it aggregates the decision trees through a voting process. Finally, it selects the prediction with the largest number of votes as the final prediction result [83].
   We apply the random forest classifier to our dataset using Python as a second method for classifying students into majors. In this experiment, we implement the random forest classifier method to compare the results with those obtained from the XGBoost method. For the random forest model, the same libraries were used as for the XGBoost classifier along with the "RandomForestClassifier". We specify the random_state parameter which is usually used to set a random subset, ensuring that the random processes within the algorithm can be reproduced [8]. An accuracy metric is used to assess the performance of the random forest model. The code to implement the random forest classifier method can be accessed via the following link: `https://github.com/hudaalsobhi/IBMM-code.git`.

Both the XGBoost and random forest models are utilized to resolve the classification issues. They are powerful classification algorithms, called classifiers, that belong to the supervised learning category of machine learning [29, 83].

3. **Light Gradient Boosting Machine (LightGBM):** LightGBM is a machine learning framework that employs gradient boosting and decision tree algorithms to accomplish a variety of tasks, such as ranking and classification. It is an enhanced version of XGBoost and possesses several advantages over its predecessor [95]. For example, LightGBM can effectively process large datasets, consume less memory, enable parallel and GPU learning, and offer faster training times while maintaining high accuracy. Additionally, it utilizes the leaf-wise algorithm to enhance its efficiency [95].
   For the third method of classifying students into majors, we use the LightGBM classifier implemented in Python. The objective in using the LightGBM method is to compare the results obtained with the XGBoost and the random forest methods. This model uses the same libraries as the XGBoost classifier as well as the "LGBMClassifier". The performance of the LightGBM model is measured using an accuracy metric. The code to implement the LightGBM classifier method can be accessed via the following link: `https://github.com/hudaalsobhi/IBMM-code.git`.

4. **Multilayer perceptron (MLP):** Multilayer perceptrons are feedforward artificial neural networks (ANNs) with multiple layers of connections [7]. There are three layers in an MLP: the input layer, the hidden layer, and the output layer. This layer has neurons with nonlinear activation functions, allowing it to handle nonlinearly separated data. A backpropagation technique is used for supervised learning during training which helps to learn relevant features automatically from the input data, saving time and possibly improving performance [7]. Choosing MLP for classification prediction problems is a good decision since it is suitable for these types of problems. Additionally, it is capable of learning nonlinear models in real-time, as well as making quick predictions [7].
   We implement multilayer perceptrons (MLP) as the fourth classification model to compare the result with the XGBoost, random forest, and LightGBM models. We apply the "MLPClassifier" using Python to predict a suitable major for each student based on the student's features. This method helps us to classify the students into their majors. We import some common libraries to train the neural network, such as MLPClassifier, Scikit-learn, and Pandas. We determine the number of nodes

(neurons) in each of the three hidden layers as 100, 50, and 25 neurons, respectively. The Adam optimizer algorithm is used to update the weights during training. The MLP model's performance is evaluated based on the accuracy metric.
The maximum number of iterations for training is set to 500 epochs to stop the training once it reaches this number. The model's performance is affected significantly by the number of epochs on which it is trained in the training dataset. Each time the model is run, its performance gradually improves as its parameters are optimized with training data [66]. To avoid underfitting and overfitting, we train the model with various numbers of epochs to find the best number of epochs to use. When the epoch number is too low, the model is underfitted, and the high epoch numbers lead to overfitting [66]. The code to implement MLP in Python with three hidden layers can be accessed via the following link: `https://github.com/hudaalsobhi/IBMM-code.git`.

6.4 Validation Process

6.4.1 Data collection, preprocessing techniques, and feature selection

This section explains the data collection process, data preprocessing techniques, and the selection of the data features.

6.4.1.1 Data collection process

We gather data online using an online survey. University students from Australia and Saudi Arabia across various academic levels, namely diploma, bachelor, master, and doctorate programs participated in this survey. The survey can be accessed via the following link: `https://bit.ly/2RrtBqI`. The collected dataset "Higher Education Students Survey" is saved as a CSV file for further analysis, and can be accessed via the following link: `https://studentutsedu-my.sharepoint.com/:f:/r/personal/hada_alsobhi_student_uts_edu_au/Documents/Datasets?csf=1&web=1&e=UNxnLq`. The following procedures were carried out to collect the data from students:

- First, we prepared online survey questions to collect academic and personal information from students.

- Second, we obtained ethical approval from the UTS Human Research Ethics Committee (HREC) under reference ETH20-4981 in 2021.

- Finally, once ethical approval had been received, we distributed the survey online, targeting both Australian and Saudi Arabian students.

As illustrated in Table 6.1, the survey consists of 12 questions for students. To address the RQ3 in this chapter, we use the data from the responses to questions 1-11. However, the data obtained in response to question 12 will be used to address RQ4, as detailed in Chapter 7.

Table 6.1: The survey questions

Questions
1. What is your gender?
2. What is your age?
3. What is the highest degree or level of education you have completed?
4. What is your current area of study (major)?
5. If you are a Master's student, what was your major during your Bachelor's degree?
6. If you are a Ph.D. student, what was your major during your Master's degree?
7. Do you want to study further?
8. If you intend to undertake further study, do you know which major you would like to take?
9. If yes, what major do you anticipate taking?
10. Have you previously completed any short learning courses?
11. If yes, in which of the following fields have you completed the short learning courses? (Select all that apply)
12. What are your top three criteria in choosing your university degree (Select all that apply)?

Based on the above survey questions, the columns that are used in the dataset are presented in Table 6.2.

Table 6.2: The columns of the dataset

Column	**Description**
Gender	string data type of three choices of gender.
Age	string data type of four choices of age range.
Highest_degree	string data type of five choices of academic degree.
Current_major	string data type of ten choices of academic major.
Bachelor_major	string data type of ten choices of academic major.
Master_major	string data type of ten choices of academic major.
Further_study	string data type of three choices of response.
Future_major	string data type of ten choices of academic major.
Short_learning_courses	string data type of thirteen choices of study area.

Table 6.3 provides information about our dataset, which includes information on 250 students who undertook their studies in Australia and Saudi Arabia. These students studied various programs, and each student's record in the dataset indicates the major that they pursued in each degree they obtained.

Of the wide range of academic majors from which to choose, we identify the 10 most commonly selected areas of study according to various surveys, namely *arts & humanities, computer science & information technology, education, engineering, medicine, pediatric*

Table 6.3: The dataset information

Dataset	**Information**
Data source	University students from Australia and Saudi Arabia
Data collection period	2021-2022
Total number of records	250
Total number of majors	10
Training data	75%
Testing data	25%

nursing, business & management, urban planning, law, and science. These majors are classes in this experiment.

6.4.1.2 Data preprocessing techniques

Preprocessing is necessary for most classification datasets before algorithms can utilize them [46]. Upon completion of the data collection, the dataset requires preprocessing to transform and reformat them into appropriate data types. Data preprocessing is crucial since real data is often incomplete and noisy [46]. The first step involves data cleaning to address missing values and remove duplicate or incomplete responses [39]. The second step is data transformation or normalization, which assigns the relevant features and involves scaling the data to ensure it falls within a specific range [39].
After data collection was complete, we used Python to analyze the dataset in depth. We use Python for data preprocessing, the most common programming language in this domain. Python has many libraries and tools designed for data handling, manipulation, and efficient preprocessing. We converted the categorical data into numerical values for the selected models to process them effectively using the "transform" method and the "LabelEncoder class". We also replaced the non-alphanumeric characters in the column names with letters. Moreover, we focused only on the necessary data, and no personal information was included to ensure that individual students could not be recognized in the research to ensure confidentiality.

To conduct classification modeling, a dataset must be obtained, and dependent or target variables must be identified to predict variables. In our experiment, the target

variables or actual values are *Future_major* column. The "Future_major" column represents the labeled column, with each row containing the target value of a specific major assigned to each student. The purpose of this step is to assign each student to one major class in the dataset, which is essential in preparing the data for ML and DL algorithms. We use these actual values to train the selected machine learning algorithms and predict accurate recommendations about the suitable major for each student.
Machine learning (ML) and deep learning (DL) algorithms are used to train each model to detect features within the labeled data, which are then used by the trained model to predict a suitable major of new student data. The selected models of both ML and DL are applied to our dataset to classify each student into one suitable major.

6.4.1.3 Selecting data features

Feature selection is a crucial technique in machine learning that aims to reduce the dimensionality of input data by selecting the most relevant features [18]. This technique can significantly improve the performance and efficiency of the model, resulting in more accurate predictions [18]. The features can be used to build ML and DL algorithms that can recommend a suitable major based on the student's data.

To extract features from the dataset, we use a combination of personal and academic background information provided by the students. Table 6.4 describes the selected features of the dataset.

6.4.2 Implementation

Following the data collection, preprocessing, and feature selection, the dataset is now ready for classification modeling.
Using Python for the implementation process, we upload the dataset which is called "Higher Education Students Survey", select the relevant features, and remove any irrelevant or redundant features to improve the efficiency and accuracy of the model. The next step is to split the dataset into two subsets: 75% for training and learning purposes and 25% for testing and verification purposes. Models are trained on a training set, and their performance is evaluated on a testing set.
To achieve accurate predictions of a student's major using a model, each selected model is trained on the input data. The dataset provides important features about the student's current majors, the majors they pursued during their bachelor's, master's, and doctoral

Table 6.4: The list of selected features

Feature	**Description**
Student_age	the student's age can help in selecting majors that are more popular among certain age groups.
Student_gender	the gender of a student can assist in identifying majors that are more popular among certain gender groups.
Current_major	the student's current major can help in selecting related majors to pursue.
Previous_majors	the student's previous majors in a bachelor's or master's degree can also assist in identifying potential areas of interest to suggest a relevant major.
Highest_degree	the student's most recent degree can also help identify their educational background and suggest a major that is suitable for their next degree.
Short_learning_courses	the micro-credentials obtained by a student in a short learning course can also be used to gain insights into their interests and areas of expertise and suggest a major that matches their skills and knowledge.
Further_study	this feature determines whether the students want to continue their studies or not. Answering yes or no can help determine whether a student intends to pursue further studies and may require recommendations about an appropriate major.
Future_major	this feature is applicable only to students who plan to pursue further studies. It can assist in identifying their expected future majors and recommending a suitable major accordingly.

degrees, their expected future majors, and the fields of their micro-credentials. The model can use these features to identify patterns and relationships that may help predict the most likely major for a given student.

After the model has completed training on the training set and has learned the patterns and relationships between the students' features and their selected majors, predictions can be made using this trained model. In the testing set, all records contain exactly

the same attributes as in the training set. During testing, the trained model uses the knowledge acquired during training. The trained model is applied to predict suitable majors for the students using the testing set. Based on the training dataset and the student's features, the model predicts the major that it assumes is most suitable for each student in the testing dataset.
Figures 6.2, 6.3, 6.4, and 6.5 present screenshots of the actual values and predicted values of the students' majors, respectively, for the XGBoost, random forest, LightGBM, and MLP model results. We compare the actual values and the predicted values to measure the accuracy and evaluate the model's performance in the following section.

6.4.3 Results and evaluation

After the trained model has predicted the suitable majors for students using the testing dataset, we evaluate the model's performance using a number of popular evaluation metrics, including accuracy, precision, recall, and F1 score. To measure the accuracy, we compare the predicted majors with the actual majors and calculate the number of correctly predicted majors. As a result, this process contributes greatly to evaluating the model's effectiveness in delivering accurate recommendations.

There were no predictions for four majors: Arts and Humanities, Education, Pediatric Nursing, and Political Science, and the prediction values produced by the trained models were 0 as shown in Tables 6.5, 6.7, 6.9, and 6.11. These values significantly affected the overall performance of the models. Consequently, we decided to exclude these majors from the evaluation and remove their values in order to increase accuracy and improve the overall model performance as shown in Tables 6.6, 6.8, 6.10, and 6.12.

Before outlining the evaluation metrics, we need to describe the confusion matrix which allows us to calculate the evaluation metrics. The confusion matrix indicates the number of correct and incorrect predicted values for each class [44]. It includes four terms: *True Positive (TP), False Positive (FP), True Negative (TN), and False Negative (FN)* [44].

- True Positive (TP): the number of correctly predicted majors of the positive class, that is, when the actual major of the dataset is positive and the predicted major is also positive.

- False Positive (FP): the number of wrongly predicted majors of the positive class, that is, when the actual major of the dataset is negative and the predicted major is positive.

- False Negative (FN): the number of correctly predicted majors of the negative class, that is, when the actual major of the dataset is positive and the predicted major is negative.

- True Negative (TN): the number of wrongly predicted majors of the negative class, that is, when the actual major of the dataset is negative and the predicted major is also negative.

The evaluation metrics are described as follows:

1. Accuracy: the percentage of correctly predicted majors of all the major classes in the dataset. It is defined as: **(TP+TN) / (TP+TN+FP+FN)** [44].

2. Precision: the percentage of correctly predicted positive majors across all positive predictions made by the model. It is defined as: **TP / (TP + FP)** [44].

3. Recall: the percentage of actual positive majors that are correctly classified by the model. It is defined as: **TP / (TP + FN)** [44].

4. F1-score: the mathematical average of precision and recall to provide a single score that represents the harmonic mean of both measures. It is defined as: **F1 score: F1 = 2 * (precision * recall) / (precision + recall)** [44].

XGBoost

Id	Future_major	Pedicted_major
117	Computer Science & Information Technology	Business & Management
9	Computer Science & Information Technology	Computer Science & Information Technology
17	Computer Science & Information Technology	Computer Science & Information Technology
20	Engineering	Engineering
125	Medicine	Medicine
6	Medicine	Computer Science & Information Technology
138	Computer Science & Information Technology	Computer Science & Information Technology
171	Computer Science & Information Technology	Arts & Humanities
131	Computer Science & Information Technology	Computer Science & Information Technology
127	Computer Science & Information Technology	Computer Science & Information Technology
104	Computer Science & Information Technology	Computer Science & Information Technology
78	Engineering	Engineering
62	Business & Management	Business & Management
146	Science	Science
184	Science	Science
151	Medicine	Medicine
45	Computer Science & Information Technology	Education
196	Computer Science & Information Technology	Computer Science & Information Technology
197	Business & Management	Computer Science & Information Technology
13	Computer Science & Information Technology	Computer Science & Information Technology
88	Business & Management	Computer Science & Information Technology
21	Medicine	Medicine
40	Science	Science
186	Medicine	Medicine
200	Science	Business & Management
54	Medicine	Medicine
183	Computer Science & Information Technology	Computer Science & Information Technology
160	Business & Management	Business & Management
108	Computer Science & Information Technology	Computer Science & Information Technology
114	Computer Science & Information Technology	Computer Science & Information Technology

Figure 6.2: Actual and predicted values of XGBoost model

Random Forest

Id	Future_major	Predicted_major
117	Computer Science & Information Technology	Business & Management
9	Computer Science & Information Technology	Computer Science & Information Technology
17	Computer Science & Information Technology	Computer Science & Information Technology
20	Engineering	Engineering
125	Medicine	Medicine
6	Medicine	Computer Science & Information Technology
138	Computer Science & Information Technology	Computer Science & Information Technology
171	Computer Science & Information Technology	Computer Science & Information Technology
131	Computer Science & Information Technology	Computer Science & Information Technology
127	Computer Science & Information Technology	Computer Science & Information Technology
104	Computer Science & Information Technology	Computer Science & Information Technology
78	Engineering	Engineering
62	Business & Management	Business & Management
146	Science	Science
184	Science	Science
151	Medicine	Medicine
45	Computer Science & Information Technology	Computer Science & Information Technology
196	Computer Science & Information Technology	Computer Science & Information Technology
197	Business & Management	Computer Science & Information Technology
13	Computer Science & Information Technology	Computer Science & Information Technology
88	Business & Management	Computer Science & Information Technology
21	Medicine	Medicine
40	Science	Science
186	Medicine	Medicine
200	Science	Science
54	Medicine	Medicine
183	Computer Science & Information Technology	Computer Science & Information Technology
160	Business & Management	Business & Management
108	Computer Science & Information Technology	Computer Science & Information Technology
114	Computer Science & Information Technology	Computer Science & Information Technology

Figure 6.3: Actual and predicted values of random forest model

LightGBM

Id	Future_major	Predicted_major
117	Computer Science & Information Technology	Engineering
9	Computer Science & Information Technology	Computer Science & Information Technology
17	Computer Science & Information Technology	Computer Science & Information Technology
20	Engineering	Engineering
125	Medicine	Science
6	Medicine	Computer Science & Information Technology
138	Computer Science & Information Technology	Computer Science & Information Technology
171	Computer Science & Information Technology	political science
131	Computer Science & Information Technology	Computer Science & Information Technology
127	Computer Science & Information Technology	Computer Science & Information Technology
104	Computer Science & Information Technology	Computer Science & Information Technology
78	Engineering	Engineering
62	Business & Management	Science
146	Science	Medicine
184	Science	Science
151	Medicine	Medicine
45	Computer Science & Information Technology	Education
196	Computer Science & Information Technology	Computer Science & Information Technology
197	Business & Management	Computer Science & Information Technology
13	Computer Science & Information Technology	Computer Science & Information Technology
88	Business & Management	Computer Science & Information Technology
21	Medicine	Science
40	Science	Science
186	Medicine	Business & Management
200	Science	Business & Management
54	Medicine	Education
183	Computer Science & Information Technology	Computer Science & Information Technology
160	Business & Management	Engineering
108	Computer Science & Information Technology	Computer Science & Information Technology
114	Computer Science & Information Technology	Computer Science & Information Technology

Figure 6.4: Actual and predicted values of LightGBM model

MLP

Id	Future_major	Predicted_major
117	Computer Science & Information Technology	Business & Management
9	Computer Science & Information Technology	Computer Science & Information Technology
17	Computer Science & Information Technology	Computer Science & Information Technology
20	Engineering	Engineering
125	Medicine	Medicine
6	Medicine	Computer Science & Information Technology
138	Computer Science & Information Technology	Computer Science & Information Technology
171	Computer Science & Information Technology	Computer Science & Information Technology
131	Computer Science & Information Technology	Computer Science & Information Technology
127	Computer Science & Information Technology	Computer Science & Information Technology
104	Computer Science & Information Technology	Computer Science & Information Technology
78	Engineering	Engineering
62	Business & Management	Business & Management
146	Science	Medicine
184	Science	Science
151	Medicine	Medicine
45	Computer Science & Information Technology	Computer Science & Information Technology
196	Computer Science & Information Technology	Computer Science & Information Technology
197	Business & Management	Computer Science & Information Technology
13	Computer Science & Information Technology	Computer Science & Information Technology
88	Business & Management	Computer Science & Information Technology
21	Medicine	Medicine
40	Science	Science
186	Medicine	Medicine
200	Science	Science
54	Medicine	Medicine
183	Computer Science & Information Technology	Science
160	Business & Management	Business & Management
108	Computer Science & Information Technology	Computer Science & Information Technology
114	Computer Science & Information Technology	Computer Science & Information Technology

Figure 6.5: Actual and predicted values of MLP model

Table 6.5: The evaluation results of the XGBoost classifier for 10 major classes

Class	**Precision**	**Recall**	**F1-score**
Business & Management	0.66	0.66	0.66
Computer Science & Information Technology	0.88	0.88	0.88
Engineering	0.66	1.00	0.80
Law	1.00	1.00	1.00
Medicine	1.00	0.77	0.87
Science	1.00	0.83	0.90
Arts & Humanities	0.000000	0.000000	0.000000
Education	0.000000	0.000000	0.000000
Pediatric Nursing	0.000000	0.000000	0.000000
Political Science	0.000000	0.000000	0.000000
Accuracy	82%		

Table 6.6: The evaluation results of the XGBoost classifier for 6 major classes

Class	**Precision**	**Recall**	**F1-score**
Business & Management	0.66	0.66	0.66
Computer Science & Information Technology	0.88	0.88	0.88
Engineering	0.66	1.00	0.80
Law	1.00	1.00	1.00
Medicine	1.00	0.77	0.87
Science	1.00	0.83	0.90
Accuracy	89%		

6.4.4 Discussion

Figures 6.6 and 6.8 show the evaluation results of all models, which include the four majors with "0" values before being excluded. Compared to the results in Figures 6.7 and 6.9, the results are significantly lower, indicating that the performance of the models has

Table 6.7: The evaluation results of the random forest classifier for 10 major classes

Class	**Precision**	**Recall**	**F1-score**
Business & Management	0.800	0.66	0.72
Computer Science & Information Technology	0.89	0.96	0.92
Engineering	0.66	1.00	0.800
Law	0.08	0.17	0.11
Medicine	1.00	0.77	0.87
Science	1.00	1.00	1.00
Arts & Humanities	0.000000	0.000000	0.000000
Education	0.000000	0.000000	0.000000
Pediatric Nursing	0.000000	0.000000	0.000000
Political Science	0.000000	0.000000	0.000000
Accuracy	86%		

Table 6.8: The evaluation results of the random forest classifier for 6 major classes

Class	**Precision**	**Recall**	**F1-score**
Business & Management	0.800	0.66	0.72
Computer Science & Information Technology	0.89	0.96	0.92
Engineering	0.66	1.00	0.800
Law	0.08	0.17	0.11
Medicine	1.00	0.77	0.87
Science	1.00	1.00	1.00
Accuracy	91%		

been adversely impacted by these values. Therefore, once these values are removed, the evaluation results dramatically increase across all models, improving the accuracy and performance of the models.

Following the removal of the zero values associated with the four majors, the accuracy of the XGBoost and LightGBM models increased by 7%, and the accuracy of the random

Table 6.9: The evaluation results of the LightGBM classifier for 10 major classes

Class	**Precision**	**Recall**	**F1-score**
Business & Management	0.33	0.17	0.22
Computer Science & Information Technology	0.88	1.00	0.94
Engineering	0.33	1.00	0.50
Law	0.12	0.10	0.20
Medicine	0.33	0.12	0.18
Science	0.33	0.40	0.36
Arts & Humanities	0.000000	0.000000	0.000000
Education	0.000000	0.000000	0.000000
Pediatric Nursing	0.000000	0.000000	0.000000
Political Science	0.000000	0.000000	0.000000
Accuracy	57%		

Table 6.10: The evaluation results of the LightGBM classifier for 6 major classes

Class	**Precision**	**Recall**	**F1-score**
Business & Management	0.33	0.17	0.22
Computer Science & Information Technology	0.88	1.00	0.94
Engineering	0.33	1.00	0.50
Law	0.12	0.10	0.20
Medicine	0.33	0.12	0.18
Science	0.33	0.40	0.36
Accuracy	64%		

forest and MLP also improved by 5%. Furthermore, all models improved significantly in precision, recall, and F1 evaluation metrics.

The results shown in Figure 6.9 indicate that there is only a minor difference in the evaluation metrics of accuracy, precision, recall, and F1-score between the XGBoost and

Table 6.11: The evaluation results of the MLP classifier for 10 major classes

Class	**Precision**	**Recall**	**F1-score**
Business & Management	1.00	0.67	0.80
Computer Science & Information Technology	0.86	1.00	0.92
Engineering	0.67	1.00	0.80
Law	0.13	0.09	0.11
Medicine	0.86	0.67	0.75
Science	1.00	0.83	0.91
Arts & Humanities	0.000000	0.000000	0.000000
Education	0.000000	0.000000	0.000000
Pediatric Nursing	0.000000	0.000000	0.000000
Political Science	0.000000	0.000000	0.000000
Accuracy	82%		

Table 6.12: The evaluation results of the MLP classifier for 6 major classes

Class	**Precision**	**Recall**	**F1-score**
Business & Management	1.00	0.67	0.80
Computer Science & Information Technology	0.86	1.00	0.92
Engineering	0.67	1.00	0.80
Law	0.13	0.09	0.11
Medicine	0.86	0.67	0.75
Science	1.00	0.83	0.91
Accuracy	87%		

random forest models, but LightGBM has the worst performance. Moreover, Figure 6.7 shows that the random forest model achieved a 2% higher accuracy compared to the XGBoost model, as the accuracy for the random forest is 91% and for XGBoost it is 89%, followed by MLP with an accuracy of 87%. This means that the random forest model is generally slightly better than XGBoost and MLP, outperforming the XGBoost model

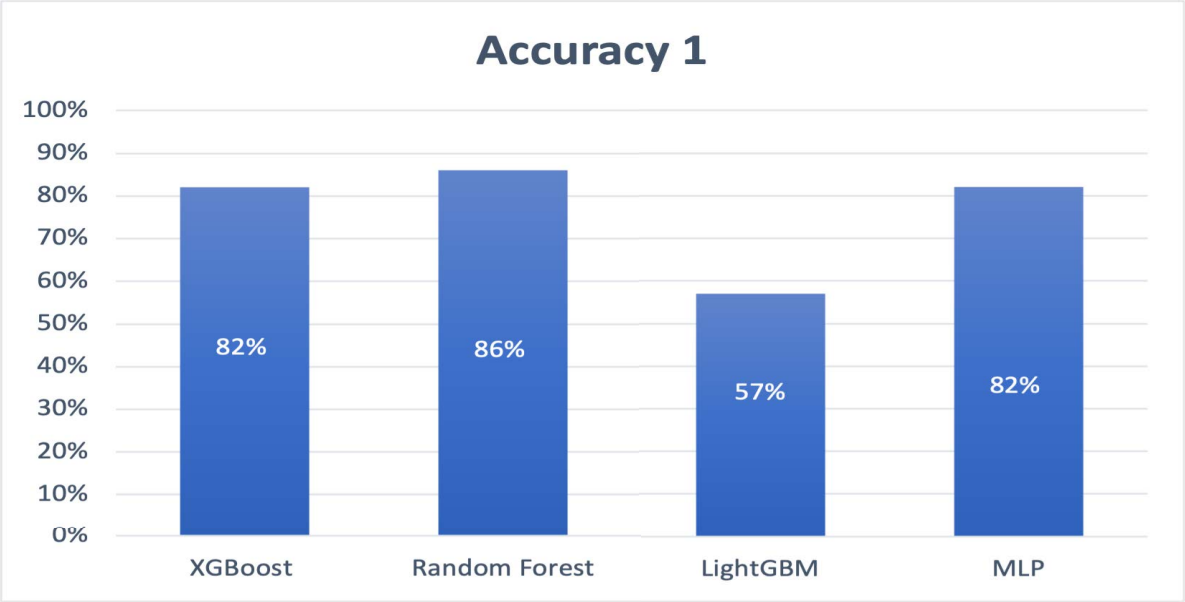

Figure 6.6: Accuracy of all models for 10 major classes

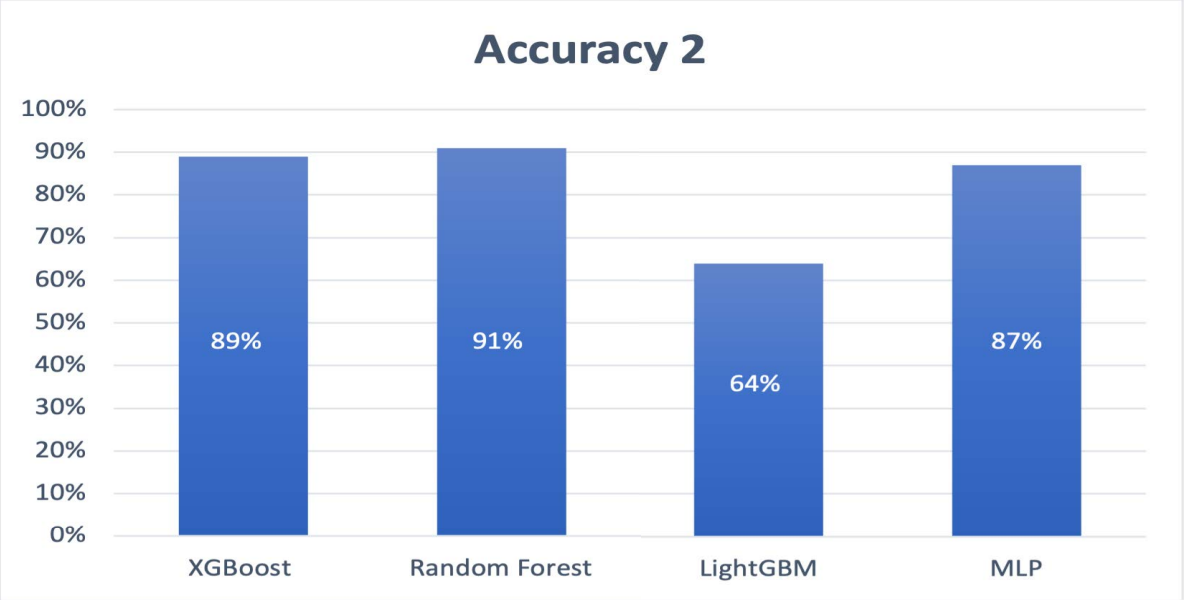

Figure 6.7: Accuracy of all models for 6 major classes

on the given dataset, and can correctly classify more cases compared to the XGBoost and MLP models. Unfortunately, the LightGBM only achieves an accuracy of 64% which indicates that it is not a good model for predicting students' majors. Ultimately, our aim is to select the model that provides the highest accuracy and best predicts the student's major which is the random forest classifier.

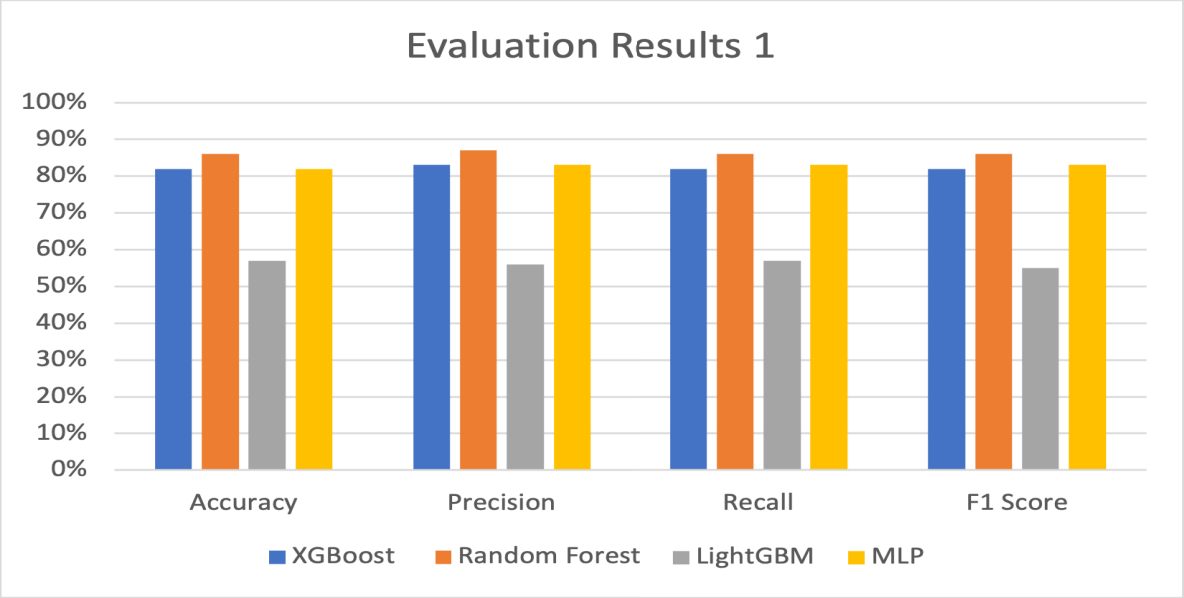

Figure 6.8: The evaluation results of all models for 10 major classes

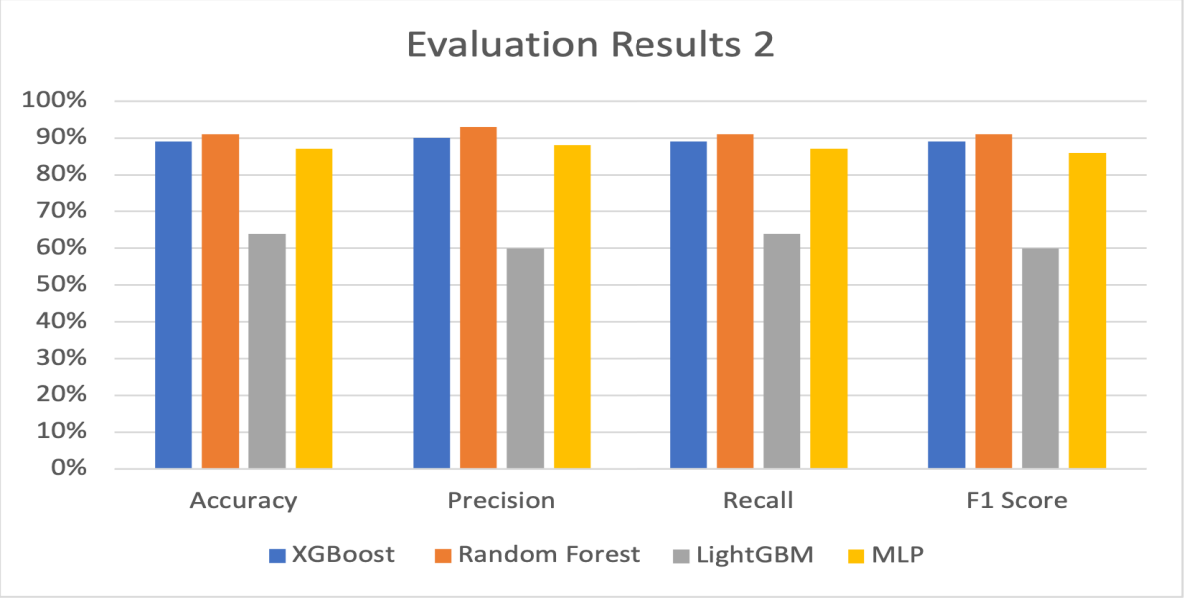

Figure 6.9: The evaluation results of all models for 6 major classes

6.5 Conclusion

In conclusion, this chapter provided a comprehensive explanation of our developed recommender system that generates personalized recommendations for students about suitable majors based on their academic profiles and micro-credentials. The selected ma-

chine learning and deep learning algorithms have been trained on our dataset, allowing them to recommend an appropriate major for students. Additionally, the implementation process and assessment outcomes of the recommender system are presented in this chapter. The proposed approach offers a practical solution to assist students in completing their degrees effectively by generating learning recommendations about their suitable academic majors. By incorporating a recommender system developed by intelligent techniques within the IBMM platform, we extend its functionality beyond credential management to assist students in selecting suitable majors aligned with their interests and career aspirations. The integration of a recommender system allows us to leverage students' verified micro-credentials and academic qualifications stored on the blockchain ledger to generate personalized recommendations for academic majors. This approach enhances the platform's utility by providing valuable guidance to students seeking assistance in identifying the most appropriate major for their degree completion.

The following chapter discusses the proposed solution to the fourth research question of this thesis, which involves gathering and selecting action plans.

CHAPTER 7

IBMM: Multi-Criteria Decision-Making Technique for Selecting the Most Suitable Action Plans

7.1 Introduction

One of the significant challenges that university students often face in the higher education environment is when they need to access and view a list of their action plans received from multiple HEIs in a unified system. A comprehensive solution that aggregates all of a student's action plans into one easily accessible view is not yet available on current e-learning platforms. Consequently, students are forced to navigate several systems and interfaces to access their action plans, causing confusion and wasted time. To address this significant gap, there is a critical need to develop a platform that can gather all action plans received from multiple HEIs into a single view.

Selecting an appropriate action plan from numerous options provided by HEIs is another challenging task that students encounter [91]. Students face considerable difficulties when evaluating and comparing these action plans based on several criteria because there is no efficient methodology. University students may be unable to choose the best action plan without being confused or dissatisfied with their choices when the methodology to support their decision-making process is inadequate [54]. Several criteria

influence students' decision-making, such as course fees, course language, university location, and university ranking [25]. This critical issue requires an intelligent decision-making technique that allows students to evaluate and select the most appropriate action plan based on various criteria [91].

In Chapter 4, a brief overview of the proposed solution for the fourth research question was presented. This solution involves the utilization of an intelligent multi-criteria decision-making technique to help students choose a suitable action plan from various options based on their preferred parameters. This chapter provides a detailed explanation of the proposed intelligent solution for the multi-criteria decision-making problem. Its objective is to help students in choosing the most optimal action plan that aligns with their preferred parameters. Moreover, this chapter introduces the suggested methodology for gathering all students' action plans on the IBMM platform and then presents an intelligent decision-making mechanism designed to help students in selecting the most optimal action plan that aligns with their preferences. This chapter presents a comprehensive explanation of the proposed solution, which involves a thorough analysis of the selection process that considers various criteria. The selection process is more intricate than collecting and viewing action plans. Hence, we discuss the methodology of predicting the most appropriate action plan for students based on their chosen criteria.

This chapter is organized as follows: Section 7.2 explains in detail the solution for gathering several action plans and selecting one based on multiple criteria, and it also presents the machine learning models used for predicting the best action plan. Section 7.3 describes the dataset used for the fourth research question, and it also presents the implementation and validation process for the selected models and the evaluation results. Finally, Section 7.4 concludes this chapter.

7.2 Solution Overview for Collecting and Selecting Action Plans

The student's ability to view and access their action plans provided by several HEIs is critical to making informed decisions during their academic journeys. Through it, they are able to compare and evaluate multiple options, comprehend course requirements, and plan their learning journey efficiently. However, choosing the right action plan is an essential decision for students as it can significantly impact their education and

future careers. Therefore, there is a need to address the multi-criteria decision-making problem that arises when students want to choose an appropriate action plan from various options based on their preferred criteria. Filtering these action plans according to students' desired criteria and recommending the most suitable action plan intelligently is an essential requirement for aiding students in the decision-making process.

This section explains the process of aggregating, storing, and displaying all the received action plans from various HEIs on the IBMM platform, and then solving the decision-making problem of selecting the most appropriate action plan from several options based on multiple criteria. As discussed in Chapter 3, one of the primary challenges students face when embarking on lifelong learning is encountering obstacles that prevent them from completing a specific degree, even though they may have accumulated various micro-credentials from different institutions, underscoring their skills, knowledge, and experience in a specific subject area. By leveraging these micro-credentials, HEIs can provide an action plan that includes the supplementary courses required for a student to complete their desired degree.

To assist students in obtaining multiple action plans from various HEIs and selecting the most suitable one based on their chosen criteria, we present our proposed solution for addressing the fourth research question, which is ***how can action plans from various educational institutions be collected to help users complete their desired degree and how can they be assisted to select an action plan based on certain preferred parameters?***

The solution for this research question is divided into two phases: the first part involves collecting, storing, and displaying all the generated action plans on the IBMM platform, while the second part focuses on selecting the most appropriate action plan based on the preferred criteria. In the following two subsections, we provide a detailed description of the solution process.

7.2.1 Collecting, storing, and viewing action plans on the IBMM

This phase is successfully implemented on the Hyperledger Fabric blockchain to collect, store, and view the students' action plans. The action plan data is handled securely and automatically using smart contracts. The outcomes of this implementation are demonstrated in Chapter 5, Section 5.6, showing the effectiveness of using blockchain

technology to maintain action plans on the IBMM platform.

In Chapter 5, we explored how the IBMM platform serves as a repository for storing a student's personal information and academic information, including their micro-credentials, learning achievements, majors, and action plans as part of their profile. In addition, we described the procedure of sharing the student's pseudonym off-chain with various HEIs to enable access to their profile and upload the student's micro-credentials and action plans. When a student identifies a suitable major through the recommender system described in Chapter 6, they can then request action plans from many HEIs.

Once HEIs have received the student's pseudonym, they have permission to access the student's profile and use the information available to create an action plan for this student. HEIs utilize the data available on the student's profile to generate an action plan that corresponds to the student's previous major, micro-credentials, and academic achievements. The process of generating the action plan takes place outside the IBMM platform. However, HEIs upload the details of the action plan onto the IBMM platform to store on the blockchain ledger as presented in Figure 5.27 in Section 5.6 in Chapter 5. The action plan data will be associated with the student's profile using their pseudonym. This linkage allows students to easily access all their action plans from different HEIs on a single view through the IBMM platform as presented in Figure 5.28 in Section 5.6 in Chapter 5. This means that the student can potentially receive multiple action plans from different HEIs, providing them with a variety of options from which to choose.
Figure 7.1 illustrates how a student's action plans are collected, stored, and viewed on the IBMM platform. The following steps outline the process of collecting, storing, and displaying multiple action plans for students from different HEIs in a unified single view that is the IBMM platform:

1. Students can apply directly to different HEIs through their websites.
2. Every HEI receives a student's application form.
3. Students share their pseudonyms with the HEIs via off-chain communication.
4. HEIs use the received pseudonym to view the student's profile on the IBMM platform.
5. Based on the information available on the student's profile, every HEI can create an action plan.

6. Every HEI uploads detailed information of the action plan onto the IBMM platform to store on the blockchain ledger.

7. Students can now access and view all the action plans they have received from every HEI via IBMM platform.

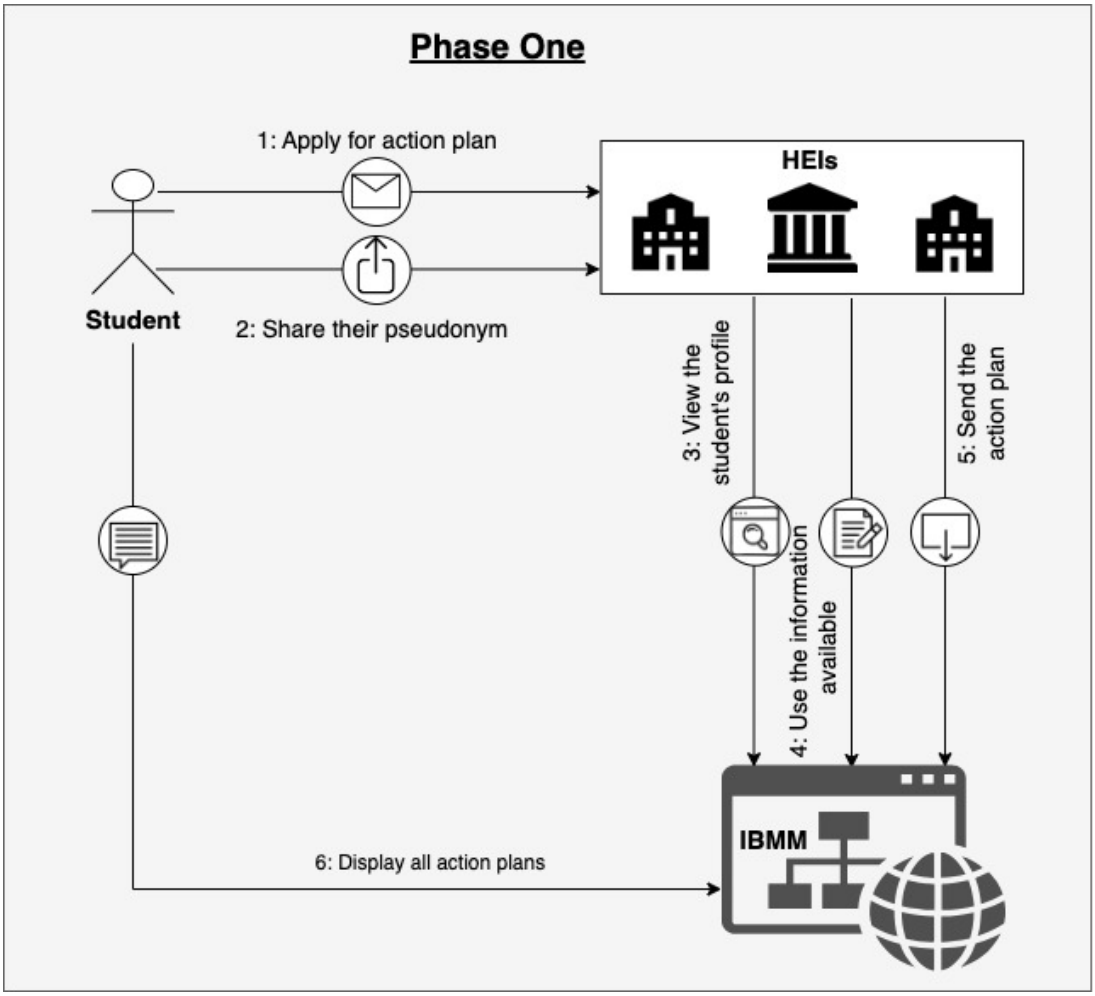

Figure 7.1: Workflow of collecting, storing, and viewing action plans process on the IBMM platform

7.2.2 Selecting the most appropriate action plan based on multiple criteria

This section describes the second phase of the proposed solution for RQ4, which is making a choice between numerous action plans based on different criteria. It provides a detailed

explanation of how we address the challenge of selecting one action plan for a student that aligns with their selected criteria. Moreover, we integrate a multi-criteria decision technique with machine learning techniques to develop an intelligent action plan selection approach that can assist students in choosing the most suitable action plan from multiple options. This intelligent technique is useful when students find it challenging to decide which of the proposed action plans best aligns with their predilection. The decision-making process for students when selecting from several action plans can be complex, due to multiple factors such as the length of the program, personal objectives, the course language, and financial considerations.

To address the decision-making problem, we implement two popular machine-learning models: XGBoost and LightGBM. In our experiment, we focused on a subset of these factors by limiting the choices in our survey question 12 to only five criteria, namely institution_rank, institution_location, course_cost, course_duration, and course_language as shown in the following link: `https://bit.ly/2RrtBqI`. The reason for using the machine-learning algorithms is to assign each student to one action plan. The following section presents the algorithms that are used for the training and testing process to select the most suitable action plan for each student.

7.2.2.1 Machine learning algorithms used in selecting an action plan

This section provides a detailed explanation of the machine learning models selected to handle the decision-making problem. We use two popular supervised machine-learning models: XGBoost and LightGBM.

XGBoost and LightGBM are two state-of-the-art boosting integrated algorithms that have gained popularity in the machine learning field in recent years. Both are based on the gradient boosting decision tree (GBDT) and are known for their high degree of accuracy and relatively short training times [95].

We use these two algorithms to rank and select the action plans, analyze and evaluate the criteria selected by the student, and then predict the most optimal action plan. These machine-learning models are trained on the training dataset. Based on the selected features, the model can be used to predict the most appropriate action plan in relation to the student's data.

XGBoost and LightGBM are effective algorithms for classification and ranking problems and can be used to accurately predict data. There are several advantages to the LightGBM and XGboost algorithms, including more accurate prediction, reduced overfitting, improved model performance and scalability, trustworthy loss functions, improved

execution speed, and quicker learning [94]. Their ranker model uses the LambdaRank algorithm which is used to minimize the pairwise loss of conducting pairwise ranking learning [77]. The following is a detailed description of each model:

1. **Extreme Gradient Boosting (XGBoost):**
   Chapter 6 covered the XGBoost model and explained its function in detail. One of the key features of XGBoost is its support for various learning objectives that can be used to train models for different ranking tasks [77]. In this method, the XGBoost library is used, which provides a variety of ranking objective functions, including (pairwise), which is frequently used for pairwise ranking. The XGBRanker is a class used for ranking tasks. We specifically focus on two objective functions that are widely used to learn ranking problems: pairwise and normalized discounted cumulative gain (NDCG) ranking, which are important tools used to efficiently optimize and implement gradient boosting [77]:

   - **Pairwise approaches:** they are widely used in Learning to Rank (LTR), which is a supervised machine learning technique that focuses on training a model to solve ranking problems [77]. The XGBoost(pairwise) ranking is the first method that is employed for ranking and selection action plans. When using the pairwise approach for ranking, the loss function of the documents is evaluated in pairs. This approach involves evaluating pairs of documents and comparing them to the true order to identify the optimal ordering [77]. Its objective is to minimize the number of ranking inversions. This method follows a natural thought process to determine the correct order and has been found to be more effective in practical applications for ranking problems. The model aims to identify the optimal order of document pairs while minimizing the objective function, as shown in the following formula [77]:

   $$\sum_{q} \sum_{i,j,l_j^q > l_j^q} l(f(x)_i^q - f(x)_j^q \tag{7.1}$$

   where l is the loss function, and *f(x)* is the predicted score or ranking for the pair.

   - **Normalized Discounted Cumulative Gain (NDCG):** it is a performance metric used to evaluate the ranking performance of a model [77]. It is calculated using a specific formula that considers the ideal order of documents and

their relevance scores, as follows [77]:

$$NDCG = \frac{DCG}{iDCG} \tag{7.2}$$

where *DCG* represents the discounted cumulative gain (DCG) at a given position, and *iDCG* represents the DCG score of the ideal order [77]. The XGBoost (NDCG) ranking is the second method used to compare the results with the XGBoost (pairwise).

The formula for NDCG incorporates DCG, which is a metric used to assess whether a model can accurately rank documents based on their relevance scores. Higher DCG scores indicate better model performance, and NDCG further standardizes these scores to ensure unbiased comparisons between different models [77]. The DCG score can be calculated at a given rank position p using the following formula [77]:

$$DCG_p = \sum_{i=1}^{p} \frac{rel_i}{log_2(i+1)} \tag{7.3}$$

where *reli* identifies the item's relevance score for its position within the ranked list at index i and *log_2(i+1)* represents the algorithm that is used as a discount factor [77].

2. **Light Gradient Boosting Machine (LightGBM):** LightGBM ranking is selected as the third method for ranking and selecting action plans, and then the results are compared with XGBoost (NCDG) and XGBoost (pairwise). LightGBM is a framework that uses gradient boosting and decision tree learning algorithms. It can perform regression, classification and ranking tasks [95]. Unlike the XGBoost algorithm, it employs a leaf-wise growth strategy to grow the tree vertically, while the XGBoost employs a level-wise strategy to grow it horizontally [94]. This method uses the LightGBM library to provide functionality for ranking.

Python is used to apply the XGBoost and LightGBM ranking to our dataset. They use some common libraries, including Pandas for data manipulation and analysis, Scikit-learn (sklearn) for splitting the dataset, and Numpy for numerical computing used to create and manipulate arrays. The following hyperparameters are set for training the model [87]:

- Tree_method: identifies the algorithm for constructing the tree.
- Booster: selects decision tree-based models as the base learners.

- Random_state: sets the random seed for reproducibility.
- Learning_rate: specifies the step size for each iteration.
- Colsample_bytree: controls the percentage of features.
- Subsample: determines the percentage of training data to be used.
- N_estimators: determines how many decision trees should be included in the ensemble.
- Max_depth: determines the maximum depth of an individual decision tree in the ensemble.

The learning rate parameter is used to prevent overfitting of the model. A small learning rate improves the accuracy of our model, so we use a learning rate of 0.1. This indicates that our model's training process has reached a stable stage at a desirable level of optimization as well as acquiring the ability to generalize effectively on the training data.

7.3 Validation Process

7.3.1 Data collection, preprocessing techniques, and feature selection

This section explains the data collection methodology, data preprocessing, and selection of data features.

7.3.1.1 Data collection and preprocessing techniques

We describe the dataset used by the three selected machine learning models to select suitable action plans for students based on multiple criteria. As detailed in Chapter 6, we collected a dataset from the students, named "Higher Education Students Survey" that contains their personal and academic information, and some selection criteria. Unfortunately, this dataset does not include the data required to select the most appropriate action plan for each student according to their selected criteria. Consequently, it became clear that there was a need for a complementary dataset that included details about the students' action plans or courses obtained from HEIs. Since no existing datasets

contained the required data, we generate a new dataset by following a methodical procedure:

1. A new dataset named "course" is manually created to provide relevant information about several courses. This dataset contains course_id, course_name, course_duration, course_cost, course_language, university_name, university_location, and university_ranking.

2. A second dataset, named "output" contains several columns from the "Higher Education Students Survey" dataset and one column from the "course" dataset. These columns are student_id, student_name, student_email address, student_gender, student_age, student_major, student_degree, and course_id. The student_name is extracted from the student_email address. The *course_id* includes two possible course options assigned to each student. In addition, one new label column is manually created and added: *enrolled_course* which includes the selected action plan/course by each student. These values are used as the actual values to compare with the predicted values and measure the accuracy.

3. Python is used to upload and process both the "course" and "output" datasets. Based on the list of the "course_id" column, we expanded each row in the "output" dataset into two rows and linked each student with two courses using an empty dataset named "df-matrix". Furthermore, two new columns are added: "is_enrolled" and "group_id". The "is_enrolled" column is added to the dataset to score each row according to two values (0 or 1). Whenever the "enrolled_course" matches the course candidate, the column is set to 1; otherwise, it is set to 0. The "group_id" column is used to group all rows with the same "student_id" in one group and the column is set to the group_number. The result of this process is to create a new dataset that provides a more detailed picture of student-course associations, and this dataset is used for all subsequent analyses and modeling.

All the datasets are saved as CSV files for further analysis and can be accessed via the following link: `https://studentutsedu-my.sharepoint.com/:f:/r/personal/hada_alsobhi_student_uts_edu_au/Documents/Datasets?csf=1&web=1&e=UNxnLq`. Once the dataset is ready, it needs to be prepared for the selected machine-learning algorithms. Python is used to remove duplicate rows from the dataset and ensure the "course_id" contains unique values. Moreover, the categorical values are converted to numerical forms, which can be used in machine learning models. In the column names, non-alphanumeric

characters are replaced by letters. The final dataset is trained and tested with Python and the results are evaluated accordingly.

7.3.1.2 Feature selection

We present the features that are used in the selected machine-learning algorithms. These features are carefully selected based on their relevance and importance in selecting the most appropriate action plan for each student. Overall, our dataset provides a comprehensive set of features for the students, including personal information, academic background, selected criteria, and action plan/course information. The selected features are detailed in Table 7.1.

In our dataset, the "course_id" column is used to link student features to the corresponding action plan/course details. The "enrolled_course" column represents the actual values for the algorithm. Every selected machine-learning model is trained to rank the list of courses that are assigned to the students. The purpose of ranking the courses is to help the algorithm select the most optimal action plan/course for a new student. By assigning two different action plans/course candidates to each student, we ensure that the recommendations for the action plans are comprehensive and well-informed. Moreover, by linking each student to their corresponding action plans, we can evaluate the effectiveness of the selected algorithms in recommending a suitable action plan. This allows us to assess the accuracy and reliability of the predictions.

7.3.2 Implementation

After preparing the dataset and selecting the relevant features, the dataset is split into two sets for testing (25%) and training (75%) purposes. Machine-learning algorithms are trained using the input features and the labeled data. Selecting the most optimal action plan/course is based on three stages of the criteria selection: first, only the institution_rank criteria; second, the institution_rank and course_cost criteria; and third, all five criteria (institution_rank, institution_location, course_cost, course_duration, and course_language). The predict function applies to each group of data, and the lambda function calculates the maximum value. The model then selects the prediction value that has the highest confidence level in every row.
The trained model now can be used as a valuable tool for selecting the most appropriate action plan for a new student based on their profile features and their selected criteria.

Table 7.1: The list of selected features

Feature	**Description**
Student_id	the identifier of each student
Student_age	the age of each student
Student_gender	the gender of each student
Student_major	the major the student is currently studying
Student_degree	the highest level of education that the student has achieved or is currently studying
Course_id	two unique identifiers for each action plan that the student has received from HEIs
Group_id	the unique identifier of each group
Enrolled_course	the course selected by the student
University_rank	criteria determining institution ranking
University_location	criteria determining the institution location
Course_cost	criteria determining the total cost of the course
Course_duration	criteria determining the duration of the course
Course_language	criteria determining the language of the course
Is_enrolled	value determining if the selected course matches one of the two options

As explained previously, each student is associated with two action plans/course candidates. We matched each one with the value in the "enrolled_course" column; if it is matched, the value is set to 1; otherwise, the value is set to 0. The values of these pairs were then grouped together. Based on this, the model calculates the predictions for each group and stores the highest one in the "predicted_course" column.
Additionally, the model calculates the predictions for each group of the original courses that are assigned to a student and stores the maximum value in the "selected_course" column. To calculate the evaluation metrics, we use the values of these two columns "predicted_course" and "selected_course" in the comparison process.

Figures 7.2, 7.3, and 7.4 show screenshots of the experiment results for the XGBoost (pairwise), XGBoost (NDCG), and LightGBM models for the specified criteria selection.

7.3.3 Results and Evaluation

This section presents the evaluation results of the selected machine-learning models. A comparison of the experiment results between XGBoost (pairwise), XGBoost (NDCG), and LightGBM is conducted to evaluate and validate the efficiency of the chosen methods in selecting the most appropriate action plan/course. We compare the predicted courses and the actual courses to measure the accuracy metric. To calculate the accuracy, the predicted courses are compared to the selected courses, and the number of correct predictions is computed. The evaluation process involves all three criteria selection stages (only the institution_rank criteria, the institution_rank and course_cost criteria, and all criteria).
We use the standard metrics commonly used to assess the performance of the machine learning models, namely accuracy, precision, recall, and F1 score. The confusion matrix (TP, TN, FP, FN) are explained in the following.

- True Positive (TP): the number of correctly predicted courses of the positive group, that is, when the actual course of the dataset is positive and the predicted course is also positive.
- False Positive (FP): the number of wrongly predicted courses of the positive group, that is, when the actual course of the dataset is negative and the predicted course is positive.
- False Negative (FN): the number of correctly predicted courses of the negative group, that is, when the actual course of the dataset is positive and the predicted course is negative.
- True Negative (TN): the number of wrongly predicted courses of the negative group, that is, when the actual course of the dataset is negative and the predicted course is also negative.

The evaluation metrics are explained as follows:

- Accuracy is the percentage of correctly predicted courses of all the courses in the dataset. It is defined as **(TP+TN) / (TP+TN+FP+FN)** [44].

- Precision is the percentage of correctly predicted positive courses across all positive predictions made by the model. It is defined as **TP / (TP + FP)** [44].

- Recall is the percentage of actual positive courses that are correctly predicted by the model. It is defined as: **TP / (TP + FN)** [44].

- F1-score is the mathematical average of precision and recall to provide a single score that represents the harmonic mean of both measures. It is defined as: **F1 score: F1 = 2 * (precision * recall) / (precision + recall)** [44].

Tables 7.2-7.10 present the performance evaluation results of each ML model for both course options (0 and 1) according to the three criteria selection stages.

XGBoost_pairwise uni_rank+course_cost

id	Selected_course	Predicted_course
12	1	1
187	1	1
265	1	1
448	0	0
624	1	1
654	1	1
712	0	0
887	1	1
1029	0	0
1070	0	0
1121	1	1
1235	1	0
1328	1	0
1513	0	0
1655	0	0
1767	0	0
1780	0	0
1829	0	1
2322	0	0
2628	0	0
2630	1	0
2757	1	1
2760	0	0
2859	0	0
2928	0	0
2933	1	1
2996	0	0

XGBoost_pairwise uni_rank_result

id	Selected_course	Predicted_course
12	1	0
187	1	1
265	1	1
448	0	0
624	1	1
654	1	1
712	0	0
887	1	1
1029	0	0
1070	0	0
1121	1	1
1235	1	0
1328	1	0
1513	0	0
1655	0	0
1767	0	0
1780	0	0
1829	0	0
2322	0	0
2628	0	0
2630	1	1
2757	1	1
2760	0	0
2859	0	0
2928	0	0
2933	1	1
2996	0	0

XGBoost_pairwise full_criteria_result

id	Selected_course	Predicted_course
12	1	0
187	1	1
265	1	1
448	0	0
624	1	1
654	1	1
712	0	0
887	1	1
1029	0	0
1070	0	0
1121	1	0
1235	1	0
1328	1	0
1513	0	0
1655	0	0
1767	0	0
1780	0	1
1829	0	0
2322	0	0
2628	0	0
2630	1	1
2757	1	0
2760	0	0
2859	0	0
2928	0	0
2933	1	1
2996	0	0

Figure 7.2: The XGBoost (pairwise) results

XGBoost_ndcg uni_rank+course_cost

id	Selected_course	Predicted_course
12	1	1
187	1	1
265	1	1
448	0	0
624	1	1
654	1	1
712	0	0
887	1	1
1029	0	0
1070	0	0
1121	1	1
1235	1	0
1328	1	0
1513	0	0
1655	0	0
1767	0	0
1780	0	1
1829	0	1
2322	0	0
2628	0	0
2630	1	0
2757	1	1
2760	0	0
2859	0	0
2928	0	0
2933	1	1
2996	0	0

XGBoost_ndcg uni_rank_result

id	Selected_course	Predicted_course
12	1	1
187	1	1
265	1	1
448	0	0
624	1	1
654	1	1
712	0	0
887	1	1
1029	0	1
1070	0	0
1121	1	0
1235	1	0
1328	1	0
1513	0	0
1655	0	0
1767	0	0
1780	0	1
1829	0	0
2322	0	0
2628	0	0
2630	1	0
2757	1	0
2760	0	0
2859	0	0
2928	0	0
2933	1	1
2996	0	0

XGBoost_ndcg full_criteria

id	Selected_course	Predicted_course
12	1	1
187	1	1
265	1	1
448	0	0
624	1	1
654	1	1
712	0	0
887	1	1
1029	0	0
1070	0	0
1121	1	0
1235	1	0
1328	1	0
1513	0	0
1655	0	0
1767	0	0
1780	0	1
1829	0	0
2322	0	0
2628	0	0
2630	1	0
2757	1	0
2760	0	0
2859	0	0
2928	0	0
2933	1	0
2996	0	0

Figure 7.3: The XGBoost (NDCG) results

Table 7.2: The XGBoost (pairwise) for criteria: institution_rank

Course-selections	**Precision**	**Recall**	**F1-score**
0	0.84	0.89	0.86
1	0.85	0.80	0.82
Accuracy	85%		

7.3.4 Discussion

Figure 7.5 compares the accuracy of the XGBoost (pairwise), XGBoost (NDCG), and LightGBM models for different criteria. The model's accuracy is evaluated on every selection criteria stage: the "institution_rank" criteria, "institution_rank + course_cost" criteria, and all criteria. XGBoost (pairwise) achieves the highest accuracy of 85% by selecting the "institution_rank" criteria or selecting the "institution_rank + course_cost"

LightGBM uni_rank+course_cost_result

id	Selected_course	Predicted_course
12	1	0
187	1	0
265	1	0
448	0	0
624	1	1
654	1	0
712	0	1
887	1	0
1029	0	1
1070	0	0
1121	1	0
1235	1	0
1328	1	0
1513	0	0
1655	0	0
1767	0	1
1780	0	1
1829	0	1
2322	0	1
2628	0	0
2630	1	1
2757	1	1
2760	0	0
2859	0	1
2928	0	0
2933	1	0
2996	0	1

LightGBM unirank_result

id	Selected_course	Predicted_course
12	1	0
187	1	0
265	1	0
448	0	0
624	1	1
654	1	0
712	0	0
887	1	0
1029	0	1
1070	0	0
1121	1	0
1235	1	0
1328	1	0
1513	0	0
1655	0	0
1767	0	1
1780	0	1
1829	0	1
2322	0	1
2628	0	0
2630	1	1
2757	1	1
2760	0	0
2859	0	0
2928	0	0
2933	1	0
2996	0	1

LightGBM full_criteria_result

id	Selected_course	Predicted_course
12	1	0
187	1	0
265	1	0
448	0	0
624	1	1
654	1	0
712	0	1
887	1	0
1029	0	1
1070	0	0
1121	1	0
1235	1	0
1328	1	0
1513	0	0
1655	0	0
1767	0	1
1780	0	1
1829	0	1
2322	0	1
2628	0	0
2630	1	1
2757	1	1
2760	0	0
2859	0	1
2928	0	0
2933	1	0
2996	0	1

Figure 7.4: The LightGBM results

Table 7.3: The XGBoost (pairwise) for criteria: institution_rank + course_cost

Course-selections	**Precision**	**Recall**	**F1-score**
0	0.88	0.83	0.85
1	0.81	0.86	0.83
Accuracy	85%		

criteria, followed by XGBoost (NDCG) which achieves 80% accuracy by selecting "institution_rank + course_cost" criteria and 79% accuracy by selecting all criteria. LightGBM has the lowest accuracy in all criteria selection stages.

Figures 7.6, 7.7, and 7.8 display the precision, recall, and F1 score of the three models for different criteria. As shown in all figures, the XGBoost (pairwise) and XGBoost (NDCG) consistently achieve the highest values, with only slight differences regardless of whether

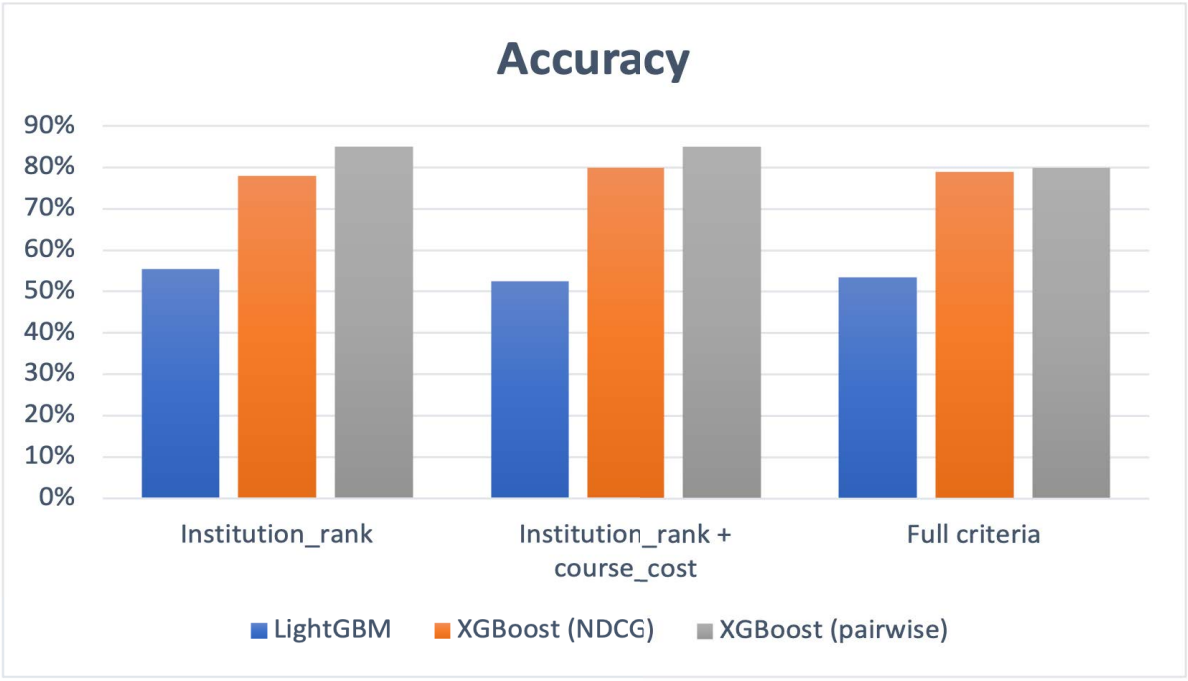

Figure 7.5: Accuracy of all models across three stages of the selected criteria

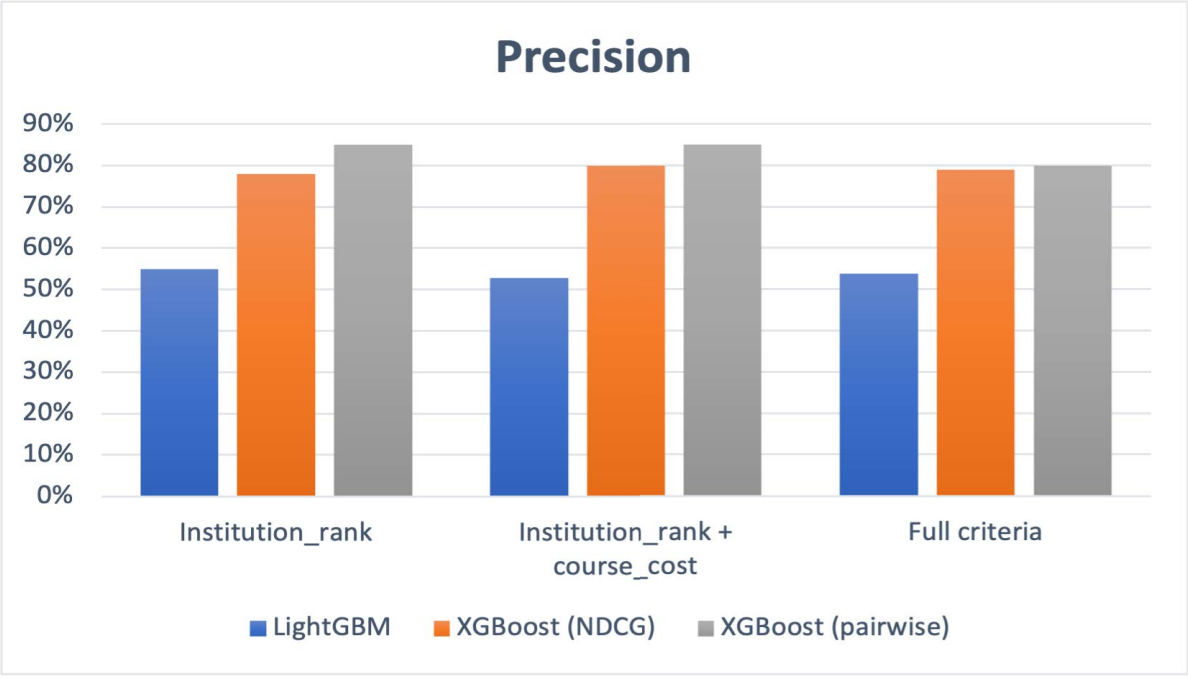

Figure 7.6: Precision of all models across three stages of the selected criteria

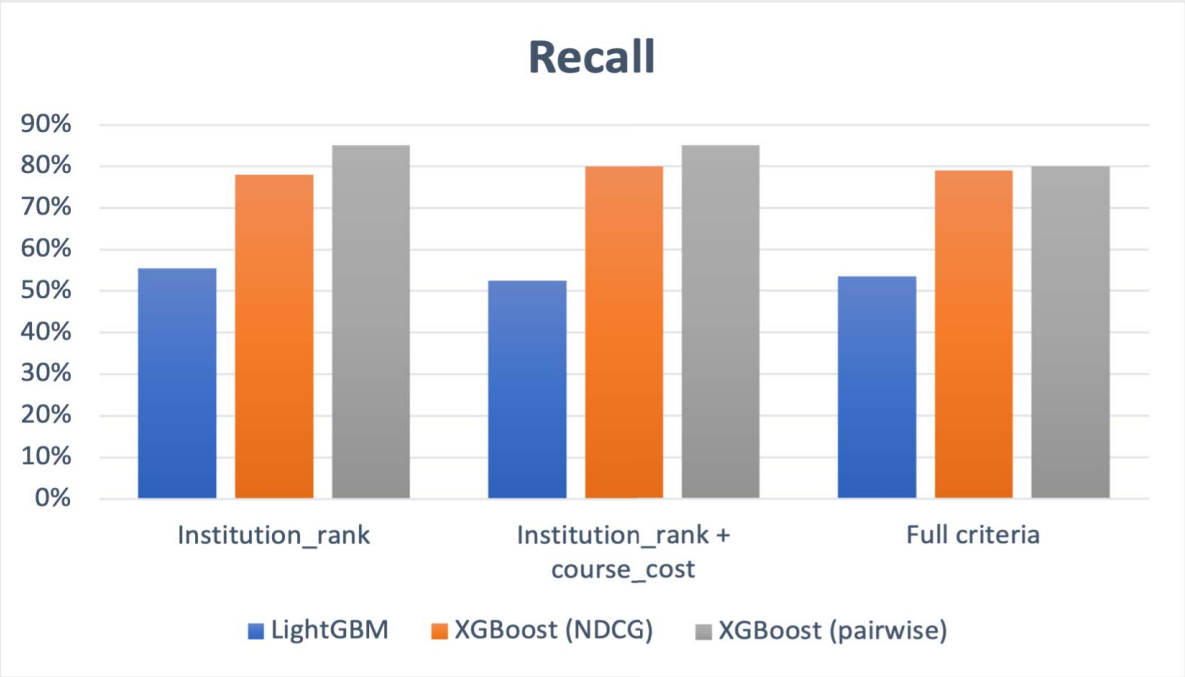

Figure 7.7: Recall of all models across three stages of the selected criteria

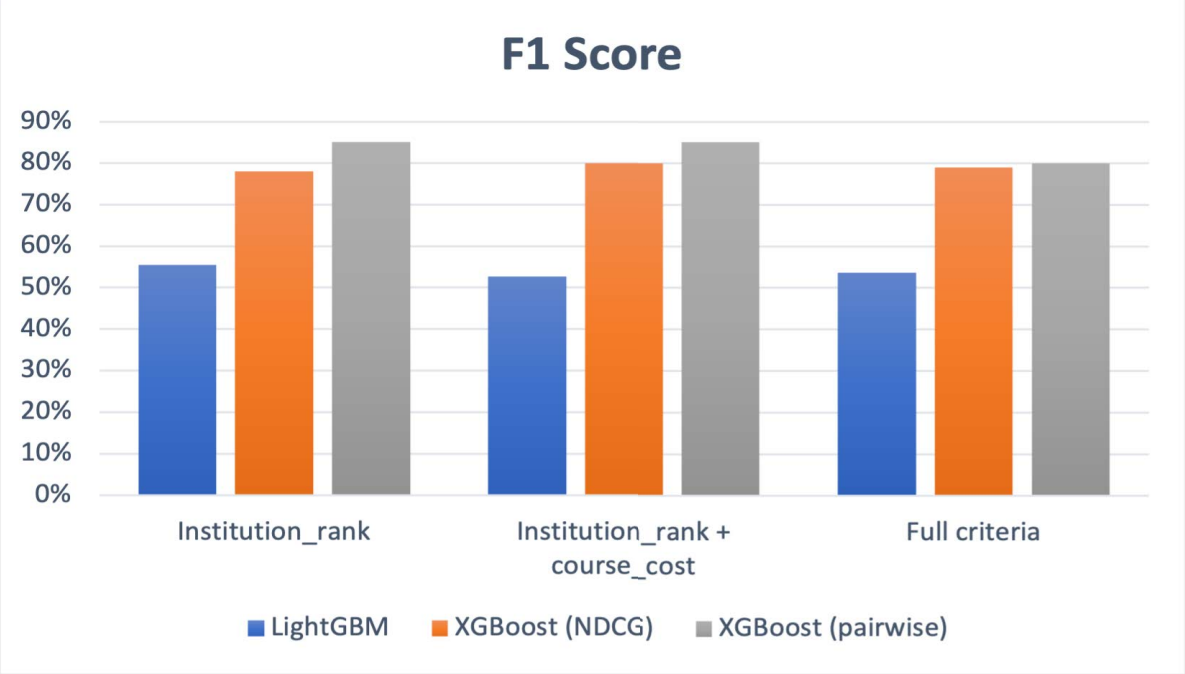

Figure 7.8: F1-Score of all models across three stages of the selected criteria

Table 7.4: The XGBoost (pairwise) for full criteria

Course-selections	**Precision**	**Recall**	**F1-score**
0	0.83	0.80	0.81
1	0.76	0.80	0.78
Accuracy	80%		

Table 7.5: The XGBoost (NDCG) for criteria: institution_rank

Course-selections	**Precision**	**Recall**	**F1-score**
0	0.81	0.78	0.79
1	0.74	0.77	0.76
Accuracy	78%		

Table 7.6: The XGBoost (NDCG) for criteria: institution_rank + course_cost

Course-selections	**Precision**	**Recall**	**F1-score**
0	0.83	0.80	0.81
1	0.76	0.80	0.78
Accuracy	80%		

the "institution_rank" only, "institution_rank + course_cost", or all criteria are considered. On the other hand, LightGBM achieves the lowest values in all criteria selection stages. Based on this analysis, we can infer that XGBoost (pairwise) and XGBoost (NDCG) are more accurate and reliable methods in selecting the most optimal action plan across multiple selection criteria.

Hence, it can be concluded that XGBoost (pairwise) is an effective approach for selecting the most suitable action plan based on multiple criteria. We use the XGBoost method with n_estimators= 110 and learning rate = 0.1 to achieve the best performance.

Table 7.7: The XGBoost (NDCG) for full criteria

Course-selections	**Precision**	**Recall**	**F1-score**
0	0.80	0.81	0.81
1	0.77	0.75	0.76
Accuracy	79%		

Table 7.8: The LightGBM for criteria: institution_rank

Course-selections	**Precision**	**Recall**	**F1-score**
0	0.60	0.62	0.61
1	0.50	0.48	0.49
Accuracy	56%		

Table 7.9: The LightGBM for criteria: institution_rank + course_cost

Course-selections	**Precision**	**Recall**	**F1-score**
0	0.58	0.55	0.56
1	0.47	0.50	0.48
Accuracy	53%		

Therefore, we choose this method as the best machine learning model, followed by XGBoost (NDCG) for recommending the most appropriate action plan for students based on their chosen criteria.

Table 7.10: The LightGBM for full criteria

Course-selections	**Precision**	**Recall**	**F1-score**
0	0.58	0.56	0.57
1	0.48	0.50	0.49
Accuracy	54%		

7.4 Conclusion

This chapter presented a comprehensive overview of the proposed solution which addresses the fourth research question of this thesis. The process of helping students collect and access all the action plans that were offered to them by several HEIs in one place is explained in this chapter. In addition, this chapter explained the intelligent action plan selection approach that was proposed to help students select the most optimal action plan/course from two available candidates based on their selected criteria. By assisting students in obtaining multiple action plans from various HEIs and selecting the most suitable one based on their criteria, our platform enhances decision-making processes. Ultimately, this approach simplifies micro-credential management, allows students to make informed decisions about their academic pathways, and builds trust in the platform's ability to facilitate academic success. This chapter also discussed the implementation and evaluation process of the selected machine-learning models for the three selection criteria stages. The performance evaluation results of the selected models are also provided.

The next chapter concludes the thesis and discusses specific areas for future research work.

CHAPTER 8

CONCLUSION AND FUTURE WORK

8.1 Introduction

This chapter presents a summary of the research findings and suggests directions for future work. Moreover, it presents an overview of the contributions made by this thesis in relation to the research objectives detailed in Chapter 3. The literature review reported in Chapter 2 indicated that several researchers have worked on blockchain-based micro-credential systems. However, none of these existing works provide a holistic platform that can store, manage, and share micro-credentials securely in a private manner, nor do they provide intelligent mechanisms for learning recommendations to help students complete their studies. Based on an investigation and the results of our systematic literature review in Chapter 2, the research gaps were identified, and we proposed a comprehensive blockchain-based solution called the Intelligent Blockchain for Managing Micro-credential (IBMM) platform for higher education students and institutions to address all the research gaps.

This chapter is structured as follows: Section 8.2 describes the research gaps that have been identified and addressed in this thesis. Section 8.3 summarizes the contributions of this thesis. The limitations are discussed in Section 8.4. Finally, Section 8.5 concludes this thesis and provides directions for future work.

8.2 Problems Addressed in this Thesis

The primary aim of this thesis is to fill the critical gaps related to managing students' micro-credentials in the higher education sector. According to the systematic literature review (SLR) discussed in Chapter 2, four research issues related to blockchain-based micro-credential systems were identified and addressed in this thesis as follows:

1. Few existing studies that provide an intelligent and trustworthy platform for managing micro-credentials in HEIs. However, none of these studies provide a holistic solution end to end that addresses all four research gaps, including sharing micro-credentials with HEIs in a privacy-preserving manner and providing learning recommendations for students about academic majors and action plans. These existing studies are only focusing on storing, managing, and sharing micro-credentials using blockchain technology.

2. None of the existing studies use a privacy-preserving technique to allow students' micro-credentials shared in a secure manner. There is no existing method that ensures the anonymity of students' identities on the blockchain while exchanging data.

3. None of the existing studies provide a recommender system to predict the appropriate major for a student to complete a certain degree based on micro-credentials. There is no intelligent technique used to recommend suitable majors for students.

4. None of the existing studies provide a mechanism to help students display all the offered action plans from many HEIs in a single view, nor is there an intelligent method to assist a student in selecting the most suitable action plan based on certain preferred criteria. There is no existing method for gathering all the action plans of multiple HEIs into one place for students to view. In addition, there is no intelligent selection method developed to assist students in selecting the best action plan.

8.3 Contributions to the Existing Literature

This section provides an overview of the thesis contributions. A major contribution of this thesis is the development of a holistic, intelligent, and trustworthy blockchain-based solution for storing, managing, and sharing micro-credentials to address the research

gaps discussed in the previous section. This thesis presents a research methodology that addresses the research questions and is divided into five chapters according to the research directions involved. The research contributions are summarized in the following sub-sections:

8.3.1 Contribution 1: Systematic literature review (SLR)

In this thesis, the current state-of-the-art literature in the area of managing micro-credentials using blockchain-based systems in higher education was comprehensively reviewed, as detailed in Chapter 2. To facilitate discussion and evaluation, we classified the existing literature into two categories based on the type of system that was proposed: (1) Intelligent platform for managing micro-credentials (IPMM) and (2) Platform for managing micro-credentials (PMM). The SLR process comprised four steps. First, the data source was selected and the search terms were identified to search for the relevant literature. Second, the search process results were screened in terms of the inclusion and exclusion criteria. Third, the filtration process was applied to the results of the previous step to select the relevant studies. Finally, the evaluation process was applied to the results of the previous step, and 15 papers were selected as relevant and were critically reviewed. This SLR identified the main shortcomings of blockchain-based micro-credential systems in higher education and found that none of the existing studies provided a comprehensive solution to assist higher education students in continuing their studies based on their micro-credentials. The SLR has been published in the Knowledge-Based Systems journal (JCR Q1, IF impact factor 8.8). The contents of this SLR are available at the following link: `https://www.sciencedirect.com/science/article/abs/pii/S095070512201334X`.

8.3.2 Contribution 2: Intelligent blockchain for managing micro-credential (IBMM) framework

This thesis develops a holistic, intelligent, and trusted platform based on blockchain technology for verifying, storing, and managing micro-credentials in higher education. Chapter 5 detailed the development of an intelligent framework for managing micro-credentials, referred to as the Intelligent Blockchain for Managing Micro-credentials (IBMM) platform. The IBMM platform assists students in sharing their micro-credentials privately with HEIs and selecting an appropriate major and action plan based on their micro-credentials to complete a specific degree. Hyperledger Fabric was used as the

foundation for developing the framework and the intelligent models were used to provide personalized recommendations. This platform can assist the stakeholders to assess and manage students' micro-credentials inside the blockchain. Furthermore, the IBMM platform is able to intelligently recommend the appropriate academic majors and action plans for the students based on their micro-credentials. The IBMM platform allows students to share their micro-credentials with several HEIs while preserving their privacy. The IBMM architecture consists of three layers: *the view layer* is the registration interface for students and HEIs, *the controller layer* performs customized actions, such as the privacy-aware sharing process, the recommender system, action plans, and intelligent action plan selection, and *the model layer* is the blockchain layer.

8.3.3 Contribution 3: Privacy-preserving mechanism to ensure the privacy of students' data

This thesis uses a privacy-preserving technique to share micro-credentials with HEIs while maintaining the privacy of students' identities on the blockchain. Using a privacy-aware sharing process facilitates efficient collaboration and micro-credential exchange among higher education institutions (HEIs), enabling a more efficient educational ecosystem. We selected a privacy-preserving technique (PPT) to securely maintain students' data and anonymity. We applied a cryptographic hashing technique to students' identities to assign a unique pseudonym to each student. With this feature, IBMM's platform allows the anonymous retrieval of student data for the users. The pseudonymization technique is used to maintain student anonymity and to improve the privacy and confidentiality of student data. Pseudonyms are used to hide the real identity of the students by replacing their real identities with pseudo-identities. As a result, we used the one-way hash function (SHA-256) to apply to the input data using the Hyperledger Fabric blockchain to generate a unique hash value with 256 bits of size which represents a pseudonym for a student. This is detailed in Chapter 5.

8.3.4 Contribution 4: Intelligent recommender system for recommending students' academic majors

This thesis develops a recommender system that generates learning recommendations for students regarding academic majors to complete a specific degree based on their micro-credentials. Chapter 6 detailed the design of an intelligent recommender system to help students find out which majors are most relevant to completing a particular degree

based on their micro-credentials. The recommender system we developed utilizes real data collected from university students to help them choose the right major based on their interests, abilities, academic qualifications, and micro-credentials. Four classification models were selected, three of which are machine learning algorithms (random forest, XGBoost, and LightGBM) and the fourth is a neural network algorithm (MLP). Classification models were used to classify each student into a single suitable major. Then, we evaluated the model's performance by comparing the predicted values with the actual values, and the number of correctly predicted majors was calculated to determine its accuracy. According to our analysis, the random forest model is the most accurate as it correctly classifies more instances compared to the other models.

8.3.5 Contribution 5: Multi-criteria decision-making technique for selecting an appropriate action plan

This thesis develops a system to enable students to access and view all their action plans provided by several HEIs in one place. Moreover, the proposed system uses an intelligent technique to identify which action plan is most appropriate for each student based on their preferred parameters. Chapter 7 details the IBMM platform which is an approach to collect, store, and present all a student's action plans that are provided by several higher education institutions (HEIs) and it also describes an intelligent decision-making mechanism to assist students in selecting the best action plan that matches their selected criteria. All student action plans were collected, stored, and viewed using the Hyperledger Fabric blockchain. In order to assist students in selecting the most suitable action plan from multiple options, we developed an intelligent selection approach based on machine learning models. A student is assigned two action plans along with three criteria options (university_rank, university_rank + course_cost, and full_criteria). Three machine learning models were chosen: XGBoost (NDCG), XGBoost (pairwise), and LightGBM. After evaluating all the models, we found that the XGBoost (pairwise) achieved the highest accuracy, so it would be ideal for selecting one action plan from multiple options in a given criteria.

8.3.6 Contribution 6: Evaluation, validation, and implementation of the proposed solutions

Each of the above contributions has been validated comprehensively using a software prototype. To evaluate the performance of the proposed framework and the privacy-

aware sharing process, we implemented it as a software prototype and tested it using the Hyperledger Fabric network, as described in Chapter 5. Moreover, as reported in Chapters 6 and 7, machine learning and artificial intelligence models were used to evaluate and test the effectiveness of the proposed solutions and the results of the recommendations for majors and action plans. This contribution is made by verifying each proposed solution for all the research objectives in order to assess their effectiveness.

8.4 Limitations

Despite our proposed approaches providing new and efficient solutions, there are some limitations that need to be improved in the future:

1. The primary limitation of this study is that it only involves a prototype system, thus requiring extensive development to transition it into a commercially viable solution that can be readily utilized by stakeholders. In the future, we need to make the prototype better at handling more users, being more reliable, and doing more things companies need. We also need to fix any technical problems, make it easier for people to use, and make sure it follows all the rules so that the system can be widely adopted and implemented effectively.

2. One other limitation of this study is that its scope only focuses on students, so the system's benefits are limited to them. By only focusing on students, the platform overlooks opportunities to provide value to other stakeholders, such as employers. If we expand the system to include better ways to verify job applicants and provide personalized job suggestions for employees, it could become more useful for everyone involved.

3. Despite our efforts to minimize bias, there might be biases in our data because most of the students who responded could be studying Computer Science & Information Technology. Also, even though we conducted surveys to collect data, differences in who responded and how many people answered could still cause bias. These biases could potentially affect the accuracy and reliability of our results, highlighting the limitations of our research.

8.5 Conclusion and Future Work

In this chapter, the thesis is concluded and some directions for future research are provided. This thesis has undertaken research involving the utilization of blockchain technology in the context of micro-credentials within higher education.
This section explores exciting future directions for work in the field of blockchain-based micro-credential management by exploring potential pathways that lie ahead. There is still wide scope for further work on this topic despite the extensive research we have conducted on the topic of this study. We intend to continue to work on this topic and inspire researchers, practitioners, and stakeholders to forge ahead and contribute to the evolution of this topic. Our future work includes but is not limited to the following:

1. By exploring interoperability between Hyperledger Fabric and other blockchain platforms, we can create a more comprehensive ecosystem for micro-credentials. We hope to implement our solution on new blockchain platforms, like Dfinity in the future and make comparisons with the Hyperledger Fabric blockchain.

2. By providing a range of privacy-enhancing options, we aim to create a secure and user-centric system that enables students to control their data and utilize innovative cryptographic and blockchain technologies. In addition to cryptography (One-way hash function (SHA-256)), we aim to implement other privacy-preserving techniques, including encryption and salting, and make comparisons between them.

3. By integrating AI and machine learning models, the platform can improve its intelligence and enhance prediction accuracy by generating learning recommendations. We intend to implement AI models alongside machine learning models to improve our developed framework and compare these models to determine which is the most accurate.

4. We plan to further enhance our recommender system to provide students with accurate predictions and recommendations for double majors in the future. We will set up a multi-label file and adapt the selected algorithms to ensure that students receive informed guidance when pursuing a more diversified education by considering the suitability and effectiveness of combining two academic majors.

5. We plan to integrate advanced verification methods and tailored analytics to facilitate an efficient and reliable assessment of job applicant's credentials. Employers

would be able to evaluate the skills and achievements of potential employees seamlessly, which would enhance the recruitment process and foster better hiring decisions. We intend to broaden the scope of our platform by including job recommendations personalized for employees.

6. Our research focused on developing the IBMM framework, conceptualizing it, and building a prototype. In the future, we plan to develop a commercial system based on the IBMM framework and turn this into a commercial reality in the future.

Bibliography

[1] (2012). Typescript is javascript with syntax for types. Available online at: https://www.typescriptlang.org/.

[2] (2017). Application guide for initial registration as a new higher education provider. Available online at: https://www.teqsa.gov.au/latest-news/publications/application-guide-initial-registration-new-higher-education-provider.

[3] (2019). Growth of international student numbers in higher education. Available online at: https://www.qs.com/growth-international-students\-higher-education/.

[4] (2021). National microcredentials framework. Available online at: https://www.dese.gov.au/higher-education-publications/resources/national-microcredentials-framework.

[5] (2022). What's new in hyperledger fabric v2.x. Available online at: https://hyperledger-fabric.readthedocs.io/en/release-2.2/whatsnew.html.

[6] (2023). Docker overview. Available online at: https://docs.docker.com/get-started/overview/.

[7] (2023). Multilayer perceptron. Available online at: https://en.wikipedia.org/wiki/Multilayer_perceptron.

[8] (2023). Xgboost. Available online at: https://www.geeksforgeeks.org/xgboost/.

[9] (2024). Blockcerts.

[10] Abba, I. V. (2022). Node.js server-side javascript - what is node used for? Available online at: https://www.freecodecamp.org/news/node-js-server-side-javascript-what-is-node-used-for/.

[11] Adem Esmail, B. and Geneletti, D. (2018). Multi-criteria decision analysis for nature conservation: A review of 20 years of applications. *Methods in Ecology and Evolution*, 9(1):42–53.

[12] Ahmat, N. H. C., Bashir, M. A. A., Razali, A. R., and Kasolang, S. (2021). Micro-credentials in higher education institutions: Challenges and opportunities. *Asian Journal of University Education*, 17(3):281–290.

[13] Akashkumar, S. (2023). Hyperledger fabric in blockchain. Available online at: `https://www.geeksforgeeks.org/hyperledger-fabric-in-blockchain/`.

[14] Al Omar, A., Rahman, M. S., Basu, A., and Kiyomoto, S. (2017). Medibchain: A blockchain based privacy preserving platform for healthcare data. In *International conference on security, privacy, and anonymity in computation, communication, and storage*, pages 534–543. Springer.

[15] Alam, S. et al. (2021). A blockchain-based framework for secure educational credentials. *Turkish Journal of Computer and Mathematics Education (TURCOMAT)*, 12(10):5157–5167.

[16] Alshaikh, K., Bahurmuz, N., Torabah, O., Alzahrani, S., Alshingiti, Z., and Meccawy, M. (2021). Using recommender systems for matching students with suitable specialization: An exploratory study at king abdulaziz university. *International Journal of Emerging Technologies in Learning (iJET)*, 16(3):316–324.

[17] Alsobhi, H. A., Alakhtar, R. A., Ubaid, A., Hussain, O. K., and Hussain, F. K. (2023). Blockchain-based micro-credentialing system in higher education institutions: Systematic literature review. *Knowledge-Based Systems*, 265:110238.

[18] Aly, M. (2005). Survey on multiclass classification methods. *Neural Netw*, 19(1-9):2.

[19] Anuvareepong, S., Phooim, S., Charoenprasoplarp, N., and Vimonratana, S. (2017). Course recommender system for student enrollment using augmented reality. In *2017 6th IIAI International Congress on Advanced Applied Informatics (IIAI-AAI)*, pages 212–217.

[20] Arenas, R. and Fernandez, P. (2018). Credenceledger: A permissioned blockchain for verifiable academic credentials. In *2018 IEEE International Conference on Engineering, Technology and Innovation (ICE/ITMC)*, pages 1–6.

[21] BANERJE, P. (2020). Lightgbm classifier in python. Available online at: https://www.kaggle.com/code/prashant111/lightgbm-classifier-in-python.

[22] Bell, A. G. (2023). An introduction to jq. Available online at: https://earthly.dev/blog/jq-select/.

[23] Bernal Bernabe, J., Canovas, J. L., Hernandez-Ramos, J. L., Torres Moreno, R., and Skarmeta, A. (2019). Privacy-preserving solutions for blockchain: Review and challenges. *IEEE Access*, 7:164908–164940.

[24] Bertram, S. and Georg, C.-P. (2018). A privacy-preserving system for data ownership using blockchain and distributed databases. *CoRR*, abs/1810.11655.

[25] Briggs, S. (2006). An exploratory study of the factors influencing undergraduate student choice: the case of higher education in scotland. *Studies in Higher Education*, 31(6):705–722.

[26] Capece, G., Levialdi Ghiron, N., and Pasquale, F. (2020). Blockchain technology: Redefining trust for digital certificates. *Sustainability*, 12(21).

[27] Chami, J. (2010). How action plans turn learning into action in the workplace. Available online at: https://guroo.pro/.

[28] Chaudhary, A., Kolhe, S., and Kamal, R. (2016). An improved random forest classifier for multi-class classification. *Information Processing in Agriculture*, 3(4):215–222.

[29] Chen, T. and Guestrin, C. (2016). Xgboost: A scalable tree boosting system. In *Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, KDD '16, pages 785–794, New York, NY, USA. Association for Computing Machinery.

[30] Choi, M., Kiran, S. R., Oh, S.-C., and Kwon, O.-Y. (2019). Blockchain-based badge award with existence proof. *Applied Sciences*, 9(12).

[31] Chukowry, V., Nanuck, G., and Sungkur, R. K. (2021). The future of continuous learning-digital badge and microcredential system using blockchain. *Global Transitions Proceedings*, 2(2):355–361. International Conference on Computing System and its Applications (ICCSA- 2021).

[32] Ciglar, C. C. (2020). Normalizing the norm of changing college majors. Available online at: https://utulsa.edu/normalizing-the-norm-of-changing-\college-majors/.

[33] contributors, W. (2023). Higher education accreditation. Available online at: https://en.wikipedia.org/wiki/Higher_education_accreditation.

[34] Crozier, R. (2022). Deakin university reveals breach of 47,000 students' details. Available online at: https://www.itnews.com.au/news/deakin-university-reveals-breach-of-47000-students-\details-582563.

[35] de Haro-Olmo, F. J., Varela-Vaca, A. J., and Alvarez-Bermejo, J. A. (2020). Blockchain from the perspective of privacy and anonymisation: A systematic literature review. *Sensors*, 20(24).

[36] Debiais-Sainton, V. (2020). European approach to micro-credentials. *EADTU Innovating Higher Education 2020 Bridging Event (I-HE2020)*.

[37] Dharmalingam, R., Ugail, H., Shivasankarappa, A. N., and Dharmalingam, V. (2022). Framework for digitally managing academic records using blockchain technology. In *Mobile Computing and Sustainable Informatics*, pages 633–645. Springer.

[38] Dinan-Thompson, M., Bajema, A., and Cowden, G. (2021). Credentialing professional learning for university educators.

[39] Fong, S. and Biuk-Aghai, R. P. (2009). An automated university admission recommender system for secondary school students. In *The 6th International Conference on Information Technology and Applications*, page 42.

[40] Ghasia, M., Machumu, H., and Smet, E. (2019). Micro-credentials in higher education institutions: An exploratory study of its place in tanzania. *International Journal of Education and Development using ICT*, 15(1).

[41] Ghonim, A. and Corpuz, I. (2021). Moving toward a digital competency-based approach in applied education: Developing a system supported by blockchain to enhance competency-based credentials. *International Journal of Higher Education*, 10(5):33–45.

[42] Gillis, A. S. (2021). What is hyperledger? everything you need to know. Available online at: https://www.techtarget.com/searchcio/definition/Hyperledger.

[43] Government, A. (2020). Course search. Available online at: https://cricos.education.gov.au/default.aspx.

[44] Grandini, M., Bagli, E., and Visani, G. (2020). Metrics for multi-class classification: an overview.

[45] Hameed, B., Khan, M. M., Noman, A., Ahmad, M. J., Talib, M. R., Ashfaq, F., Usman, H., and Yousaf, M. (2019). A review of blockchain based educational projects. *International Journal of Advanced Computer Science and Applications*, 10(10).

[46] Han, J., Kamber, M., and Pei, J. (2012). *Data mining concepts and techniques third edition*. Morgan kaufmann.

[47] Hanafy, A. (2020). Features and affordances of micro-credential platforms in higher education. Master's thesis.

[48] Herrity, J. (2023). How to write an action plan (with template and example). Available online at: https://www.indeed.com/career-advice/career-development/how-to-write-an-action-plan.

[49] Holbl, M., Kamisalic, A., Turkanovic, M., Kompara, M., Podgorelec, B., and Hericko, M. (2018). Eductx: An ecosystem for managing digital micro-credentials. In *2018 28th EAEEIE Annual Conference (EAEEIE)*, pages 1–9.

[50] Howell, M. (2009). Homebrew (package manager). Available online at: https://en.wikipedia.org/wiki/Homebrew_(package_manager).

[51] 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.

[52] Jones-Esan, L. J., Nadda, V., and Albright, K. S. (2022). *Knowledge Management and Research Innovation in Global Higher Education Institutions*. IGI Global.

[53] Kargin, A. (2020). Academic degrees. Available online at: https://www.unipage.net/en/degrees_academic.

[54] Karp, M. J. M. (2013). Entering a program: Helping students make academic and career decisions.

[55] Kato, S., Galan-Muros, V., and Weko, T. (2020). The emergence of alternative credentials. (216).

[56] Ken Peffers, Tuure Tuunanen, M. A. R. and Chatterjee, S. (2007). A design science research methodology for information systems research. *Journal of Management Information Systems*, 24(3):45–77.

[57] Khadka, N. (2023). Lightgbm algorithm: The key to winning machine learning competitions. Available online at: `https://dataaspirant.com/lightgbm-algorithm/`.

[58] Kishore, S., Chan, J., Muthupoltotage, U. P., Young, N., and Sundaram, D. (2021). Blockchain-based micro-credentials: Design, implementation, evaluation and adoption. In *Hawaii International Conference on System Sciences*. Hawaii International Conference on System Sciences.

[59] Kumar, R., Pattnaik, P. K., and Pandey, P. (2017). Secure data analysis in clusters (iris database). In *Handbook of Research on Advanced Data Mining Techniques and Applications for Business Intelligence*, pages 52–61. IGI Global.

[60] Kumaresh, S. (2021). Academic blockchain: An application of blockchain technology in education system. In *Data Management, Analytics and Innovation*, pages 435–448. Springer.

[61] Kusic, Sinisa, S. V. and Zovko, A. (2022). Micro-credentials-improvement or fragmentation in higher education?

[62] Li, Z. and Ma, Z. (2021). A blockchain-based credible and secure education experience data management scheme supporting for searchable encryption. *China Communications*, 18(6):172–183.

[63] Lim, C. L., Nair, P. K., Keppell, M. J., Hassan, N., and Ayub, E. (2018). Developing a framework for the university-wide implementation of micro-credentials and digital badges: A case study from a malaysian private university. In *2018 IEEE 4th International Conference on Computer and Communications (ICCC)*, pages 1715–1719.

[64] Machashtchik, P. and Britchenko, I. (2017). Prospects of innovative technologies into educational system introduction.

[65] Mainetti, L., Paiano, R., Pedone, M., Quarta, M., and Dervishi, E. (2022). Digital brick: Enhancing the student experience using blockchain, open badges and recommendations. *Education Sciences*, 12(8).

[66] Michelucci, U. (2022). *Applied Deep Learning with TensorFlow 2: Learn to Implement Advanced Deep Learning Techniques with Python*. Springer.

[67] Mikroyannidis, A. (2020). Blockchain applications in education: A case study in lifelong learning. In *The 12th International Conference on Mobile, Hybrid, and On-line Learning (eLmL 2020)*.

[68] Mikroyannidis, A., Domingue, J., Bachler, M., and Quick, K. (2018a). A learner-centred approach for lifelong learning powered by the blockchain. In Bastiaens, T., Braak, J. V., Brown, M., Cantoni, L., Castro, M., Christensen, R., Davidson-Shivers, G. V., DePryck, K., Ebner, M., Fominykh, M., Fulford, C., Hatzipanagos, S., Knezek, G., Kreijns, K., Marks, G., Sointu, E., Sorensen, E. K., Viteli, J., Voogt, J., Weber, P., Weippl, E., and Zawacki-Richter, O., editors, *Proceedings of EdMedia + Innovate Learning 2018*, pages 1388–1393, Amsterdam, Netherlands. Association for the Advancement of Computing in Education (AACE).

[69] Mikroyannidis, A., Domingue, J., Bachler, M., and Quick, K. (2018b). Smart blockchain badges for data science education. In *2018 IEEE Frontiers in Education Conference (FIE)*, pages 1–5.

[70] Mikroyannidis, A., Third, A., Chowdhury, N., Bachler, M., and Domingue, J. (2020a). Supporting lifelong learning with smart blockchain badges. *International Journal On Advances in Intelligent Systems*, 13(3 & 4):163–176.

[71] Mikroyannidis, A., Third, A., and Domingue, J. (2020b). A case study on the decentralisation of lifelong learning using blockchain technology. *Journal of Interactive Media in Education*, 2020(1):1–10.

[72] Moldoff, D. (2006). What is a college major. Available online at: `https://www.collegetransfer.net/AskCT/What-is-a-College-Major`.

[73] Patel, V., Khatiwala, F., Shah, K., and Choksi, Y. (2020). A review on blockchain technology: Components, issues and challenges. In Kumar, A., Paprzycki, M., and Gunjan, V. K., editors, *ICDSMLA 2019*, pages 1257–1262, Singapore. Springer Singapore.

[74] Patnaik, P. (2022). Personalized product recommendation and user satisfaction: Theory and application. In *Management Strategies for Sustainability, New Knowledge Innovation, and Personalized Products and Services*, pages 35–67. IGI Global.

[75] Perveez, S. H. (2023). What is git: Features, command and workflow in git. Available online at: https://www.simplilearn.com/tutorials/git-tutorial/what-is-git.

[76] Poudel, U. and Gajjela, S. (2019). *A BLOCKCHAIN BASED MICRO-CREDENTIALING SYSTEM*. PhD thesis.

[77] Qomariyah, N. N., Kazakov, D., and Fajar, A. N. (2020). Predicting user preferences with xgboost learning to rank method. In *2020 3rd International Seminar on Research of Information Technology and Intelligent Systems (ISRITI)*, pages 123–128.

[78] Quantin, C., Bouzelat, H., Allaert, F., Benhamiche, A., Faivre, J., and Dusserre, L. (1998). How to ensure data security of an epidemiological follow-up:quality assessment of an anonymous record linkage procedure. *International Journal of Medical Informatics*, 49(1):117–122.

[79] Sadiku, M. N., Eze, K. G., and Musa, S. M. (2018). Smart contracts: A primer. *Journal of Scientific and Engineering Research*, 5(5):538–541.

[80] Sareen, S. (2018). Curl. Available online at: https://medium.com/@shivangisareen/curl-10055699d13d.

[81] satota and denyeart (2019). Hyperledger/fabric-samples: Samples for hyperledger fabric. Available online at: https://github.com/hyperledger/fabric-samples.

[82] Shen, C. and Pena-Mora, F. (2018). Blockchain for cities‚Äîa systematic literature review. *IEEE Access*, 6:76787–76819.

[83] Simplilearn (2023a). Random forest algorithm. Available online at: https://www.simplilearn.com/tutorials/machine-learning-tutorial/random-forest-algorithm.

[84] Simplilearn, S. (2023b). What is xgboost? an introduction to xgboost algorithm in machine learning. Available online at: https://www.simplilearn.com/what-is-xgboost-algorithm-in-machine-learning-article.

[85] Singh, L. B., Chaturvedi, R. K., Mehdi, S. A., and Srivastava, S. (2020). Student's preference towards specialization selection: An exploratory perspective. *ADHYAYAN: A JOURNAL OF MANAGEMENT SCIENCES*, 10(02):10–16.

[86] 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.

[87] Sureshmecad, A. (2021). Xgboost hyperparameter-autompg. Available online at: `https://www.kaggle.com/code/sureshmecad/xgboost-hyperparameter-autompg`.

[88] Terzi, S., Ioannis, S., Votis, K., and Tsiatsos, T. (2022). A life-long learning education passport powered by blockchain technology and verifiable digital credentials: The blockademic project. In *International Conference on Software Engineering and Formal Methods*, pages 249–263. Springer.

[89] Turkanovic, M., Holbl, M., Kosifç, K., Hericko, M., and Kamisalic, A. (2018). Eductx: A blockchain-based higher education credit platform. *IEEE Access*, 6:5112–5127.

[90] Vaishali (2020). Xcode command-line tools. Available online at: `https://medium.com/ivaishali/xcode-command-line-tools-26f95ba6fb71`.

[91] Wongvilaisakul, W., Netinant, P., and Rukhiran, M. (2023). Dynamic multi-criteria decision making of graduate admission recommender system: Ahp and fuzzy ahp approaches. *Sustainability*, 15(12).

[92] Wust, K. and Gervais, A. (2018). Do you need a blockchain? In *2018 Crypto Valley Conference on Blockchain Technology (CVCBT)*, pages 45–54.

[93] Yaga, D., Mell, P., Roby, N., and Scarfone, K. (2019). Blockchain technology overview. *CoRR*, abs/1906.11078. Available online at: `http://arxiv.org/abs/1906.11078`.

[94] Yao, X., Fu, X., and Zong, C. (2022). Short-term load forecasting method based on feature preference strategy and lightgbm-xgboost. *IEEE Access*, 10:75257–75268.

[95] Zhang, D. and Gong, Y. (2020). The comparison of lightgbm and xgboost coupling factor analysis and prediagnosis of acute liver failure. *IEEE Access*, 8:220990–221003.

[96] Zheng, Z., Xie, S., Dai, H., Chen, X., and Wang, H. (2017). An overview of blockchain technology: Architecture, consensus, and future trends. In *2017 IEEE International Congress on Big Data (BigData Congress)*, pages 557–564.