MAKERERE UNIVERSITY

COLLEGE OF COMPUTING & INFORMATION SCIENCES

STORAGE OF ACADEMIC RECORDS USING BLOCKCHAIN TECHNOLOGY

By
CSC 19-03

DEPARTMENT OF COMPUTER SCIENCE

SCHOOL OF COMPUTING AND INFORMATICS TECHNOLOGY

A Project report Submitted to the School of Computing and Informatics Technology For the Study Leading to a Project Report in Partial Fulfillment of the Requirements for the Award of the Degree of Bachelor of Science in Computer Science Of Makerere University

Supervisor: Prof. Engineer Bainomugisha

Department of Computer Science
School of Computing and Informatics Technology, Makerere University
baino@cis.mak.ac.ug

April, 2019

Declaration

We Group CSC 19-3 do hereby declare that this Project Report is original and has not been published and/or submitted for any other degree award to any other University before.

GROUP MEMBERSHIP			
No.	Name	Registration Number	Signature
1	Araka Stephen Gift Mukoya	16/K/2148/EVE	
2	Agwa Daniel	16/U/2872/EVE	
3	Omoding John	16/U/11013/EVE	
4	Wafula Derrick	16/U/20275/EVE	

Approval

This Project Report has been submitted for examination with the approval of the following supervisor.

Professor Engineer Bainomugisha
BSc. CS, MSc. CS,
School of Computing & IT
College of Computing & IT
Makerere University
baino@cis.mak.ac.ug

Signed: _____

Date: _____

Dedication

We dedicate this report to the Almighty God without whom we can do nothing. We further dedicate it to our parents and guardians for their unceasing and selfless support throughout our stay in this university.

Acknowledgement

We are deeply indebted to our project supervisor Professor Engineer Bainomugisha whose unlimited steadfast support, expertise and inspirations has made this project a great success. In a very special way, we thank him for every support he has rendered unto us to see that we succeed in this challenging study.

Special thanks go to our friends and families who have contained the hectic moments and stress we have been through during the course of the research project.

We thank the school for giving us the grand opportunity to work as a team which has indeed promoted our team work spirit and communication skills. We also thank individual group members for the good team spirit and solidarity.

Abstract

Storage of Academic Documents using Blockchain arose after the realization of the bureaucracy and loopholes involved in obtaining academic records in educational institutions all over the country. The application is aimed at ensuring easy access, distribution and security of academic transcripts attained by students.

Contents

List of Figures

List of Tables

Chapter 1

Introduction

1.1 Background

There have been efforts to streamline delivery of authentic information about students who attend higher institutions of learning.

In a bid to achieve this, Makerere University, like any other institutions, uses a conventional online system to manage students' results. Upon admission to the university, an account is opened for each student through which they can can view their progressive academic records which are uploaded by a centralized administration that comprises of the school registrars. For security purposes, users are required to enter credentials i.e Student Number / Registration Number and Password. Through this, only authentic users can access the system. The use of this online system has eased students' access to their records as opposed to the formally crowded notice boards where results were pinned. For purposes of security, the system runs on the university's intranet network.

Upon completion of their study at the University, students' are awarded with an inventory of the courses taken and grades earned throughout their course of study. This comes in the form of an academic transcript. However, since the issued transcript is in hard copy, this comes with a number of complications. For example security risks, duplication and forgery, ease of access and distribution.

Recently one of the breakthroughs in technology has been the management of records belonging to a group of people using a decentralized system. One may wonder how this is possible. Well, this is done using a technology known as blockchain.

A blockchain is a growing list of records which are linked using cryptography[1]. Blockchain can not only be used to store records, but also be used for their secure manipulation. By design, a blockchain is resistant to modification of the

data stored on it. It is "an open, distributed ledger that can record transactions between two parties efficiently and in a verifiable and permanent way".

In the context of Makerere University for example, blockchain technology would be a good alternative to storing syudents' transcripts. In addition to issuing transcripts in hard copy form, using blockchain guarantees one some extra features that would better the management and storage of students' records. For example [2] :

Transparency Both parties who are interested in viewing academic credentials can see them on the blockchain. This ensures that only people with ownership rights can make decisions about who has access to particular information.

Immutability Blockchains are the most secure source for storing the information right now. They rely on the integrity of the network to ensure the authenticity of the stored information. Thus, academic certificates stored on the blockchain are immutable.

Disintermediation - Using the blockchain to store and share academic credentials helps us bypass the need for a central controlling authority that manages and keeps records. This makes the overall process of storing credentials more trustworthy as there are no middlemen involved.

Collaboration Once the information becomes available on the blockchain, it is much easier to ascribe ownership, and therefore safer to share the information without the fear of this information being compromised.

In this project, we intend to build a blockchain application that will aid the management of students' records at Makerere University.

1.2 Problem Statement

In an article published by the Daily Monitor in March 2017, 87 per cent of graduates cannot find jobs. "According to National Planning Authority (NPA) statistics released from [6 12, March 2017], 700,000 people join the job market every year regardless of qualification but only 90,000 get something to do."[4] One of the major causes of this is the problem of fake academic papers. It is a well-known secret that while a considerable number of Ugandans tender in doctored documents to get employment, a huge number of people with genuine papers remain unemployed.

Currently, it is pretty easy to obtain a forged transcript. For as little as $100, one can acquire a fake transcript that required another person four years of study. Unfortunately for employers, it is not so obvious to tell the difference between authentic and counterfeit.

This project aims at tackling the above-mentioned shortcoming with a focus on the results testimonial issued to a student of the university. Enforcing means of verification of academic documents is our proposed approach to reducing these rates of unemployment, especially for university graduates.

1.3 Main Objective

The overall aim of this project is to improve authenticity of documents by implementing block chain technology.

1.3.1 Specific Objectives

The specific objectives of the study were:

- To de-materialize academic documents. Unlike paper-based records that can easily get lost, once put in block chain, the students' grades will be safe.
- To reduce the need for a third-party controlling authority that manages and keeps students' records.

1.3.2 Scope

The challenges mentioned in the problem statement above are broad and cut across a number of institutions of higher learning in the nation and even beyond borders. For this project however, the focus will be on Makerere University Main Campus located in Kampala, Uganda. Furthermore, the project will focus on issuance of the academic transcript issued to a student of the university among other documents.

1.3.3 Significance

No one would like to eat half baked bread leave alone the raw dough. The employment industry is flooded with so many employees that have barely attained the knowledge to perform the tasks they are given simply because they were able to manipulate their results and convince their employer that theyre capable.

This project is aimed at closing such loop holes that allow people manipulate their results. This would allow an employer attain all the necessary information about his/her employees as all the information will appear on a block chain network.

Besides authentic results, the load of paperwork will be cut by a great deal. This

is the documents shall be issued electronically as opposed to manual issuance. Generally, this would ease records keeping and reduce the work currently involved.

For employers, block chain technology will avoid them having to spend valuable time checking candidates' educational credentials by having to call universities or to pay a third party to do the job.

By authenticity of academic records, Makerere University will exist in accordance to its values and reflect these values. Through this, the university will embrace the added responsibility of leading by example not only as the best university in Uganda, but also to the worldwide community of institutions of higher learning.

Chapter 2

Literature Review

2.1 Background

Storing and verifying students' academic transcripts can be costly and time-consuming for academia, students and businesses alike. Through this project, we look to turn to blockchain technology for a solution. But first of all, let us start with a review of the blockchain technology and its current applications.

2.1.1 Review of Existing System

At Makerere University, there is a system that has been developed for the purpose of storage of students results. The table below summarizes a review of the existing system.

Results System	Strength	Weakness
Web URL - www.ar.mak.ac.ug **Security:** Despite deployment on an intranet, the system is not secure. It is still susceptible to external threats from hackers or malicious software including worms, viruses, and malware. It could also be subject to internal threats from the users, since it doesnt cater for issues like weak passwords and access control [4].	**Reliable:** students are able to access their marks online and follow up in case of any fault.	**Limited access:** Access is limited to the universitys intranet.

A review of the proposed system

Considering the flaws of the current system, we take a brief look into how blockchain technology could provide a solution to the above-mentioned weaknesses.

Blockchain works like a decentralized ledger, storing information on a global network that is publicly available and should be safe from tampering. Henri Pihkala, founder and CEO of Streamr, a block chain-based platform for live data streams, captures the paradox: *"we make a central place which is decentralized."*

It is an interesting technological innovation that has clearly caught the publics imagination. But how does it matter to the educational ecosystem?

Any operation as large and distributed as education in 2018 will find a use for blockchain technology. Educational institutions like universities are large-scale, multi-institutional operations that run on the whims and fancies of many moving parts their stakeholders. Running such institutions is not a simple process, but it can be made simpler through the use of blockchain. Described

below are not only some of the contributions, but also weaknesses and gaps that are associated with this technology.

Contributions

Because decentralized applications run on the block chain, they benefit from all of its properties, which include:-

- **Immutability** A third party cannot make any changes to data.
- **Corruption & tamper proof** Apps are based on a network formed around the principle of consensus, making censorship impossible.
- **Secure** With no central point of failure and secured using cryptography, applications are well protected against hacking attacks and fraudulent activities.
- **Zero downtime** Apps never go down and can never be switched off.

For an example of the contribution of this technology, we look at the University of Nicosia in Cyprus, which is using the technology to record students' achievements. According to George Papageorgiou, a digital currency lecturer at the university, the technology is proving popular. He had this to say to CNBC News:
"We've only encountered enthusiasm in the practical uses so far and students are glad to be able to verify, with their new knowledge and the blockchain, that their digital certificate is genuine and that it cannot be recreated. We believe this instills confidence in both students and potential employers that (they) can check on their own, whether a presented certificate is real or not".[5]

This is proof that the implementation is already reaping fruits in some institutions around the world.

Weaknesses and gaps

However, despite all the possibilities offered by blockchain, there have been various challenges associated with it.

We observe challenges in both the perspective of the end-user, and we, the researchers. From the users view, according to Donald Clark [6], an EdTech entrepreneur and advisor of EdTech companies, some public sector organizations just dont like the innovation and stick to their institutional silos. This is basically because the technology has not been around for a long time which makes many potential users have doubts about its possibilities. To overcome this, we intend to train the parties in these institutions on how to use this technology and also show them the advantages.

From our research perspective, the major challenge is that the subject of study is of a relatively early stage. Blockchain technologies are under active development globally, and there may be recent advances that impact our findings.

In conclusion, it is important to note that blockchain is a technology that clearly has applications in the world of learning at individual, institutional and international levels. It is relevant in all sorts of contexts: schools, colleges, universities among others.

One thing we know for sure is that students have their eyes open and are looking for alternatives. Perhaps, like Bitcoin, the blockchain revolution will ultimately come from left of field.

Chapter 3

Methodology

3.1 Introduction

This chapter contains a description of the techniques, methods and tools used during the research process. Also contained in this chapter, is a description of the implementation, testing and validation of the system.

3.2 Data Collection

The data collection process in this project was done through interviews with the various stakeholders of the system for example the students and administrative assistants at different colleges of the university. Document reviews were also done in the process of data collection.

From the vast number of stakeholders, sampling was done using the systematic sampling technique. This is a type of probability sampling where every element of the sample space has an equal chance of being picked.

3.2.1 Interviews

This is a one to one discussion between the project team and the expected users of the system. An advantage this method has over many others is that the interviewer gets first-hand information. This method is also qualitative in nature and helpful in validating the already gathered information. However, there is a possibility of the interviewee giving false information regarding particular aspects based on their emotional state.

The interviews were carried through a one on one discussion with the interviewees.

Reasons for using this method

- Quick feedback from respondents cuts short on the time of requirements collections.
- There is a possibility of asking questions that are not included in the interview script.
- This technique allows respondents to describe what is more important to them.

3.2.2 Observation

As a source of additional information, we carried out some observations of the current results management system used by the university. This, we did by accessing the student portal(ar.mak.ac.ug)used for results.

The major aim for our observations was to get qualitative information about the existing system that handles students results.

Reasons for using this method

- Provides access to situations and people where questionnaires and interviews are inappropriate to use.
- Strong on validity and in-depth understanding of the design problem.
- Good for explaining meaning and context.

3.2.3 Document Review

Through literature review, we collected information from already existing related research. This research was done on similar systems to the one involved in this project that already exist. This information was gathered from online sources like the internet, journals an and other relevant materials on the problem domain from libraries around the university.

3.3 Tools

We used notebooks and pens to note down information obtained during the interviews. I addition, we also used smartphones to record the conversations. tabulated below is a summary of the methods used in the data collection process and tools used to implement them.

Table 3.1: Methods and tools

Method	**Tools**
Interviews	• Interview guide • Pens and notebooks • Smartphones
Observations	• Personal Computers • Smartphones • Internet
Document Review	• Books • Articles

3.4 Data Analysis

The collected data was analyzed to be able to attain consistency and reliability for proper modeling and implementation of the system. The data was studied to identify key user and system requirements. These were classified under functional and non-functional requirements.

3.5 System Design and Implementation

In order to achieve efficient project management, we adapted the agile software development methodology where the requirements and solutions evolve together throughout the development process. This approach significantly contributed to the success of the project because we were able to anticipate the need for flexibility in time.

3.5.1 System Design

The system was designed using use case and data flow diagrams. The generated use case diagram visually express how the different users interact with the system and the data flow diagrams showed how data flows through the system.

In the development of the use cases, we used the object-oriented analysis devel-

opment method to design the system. In this phase, we determined the systems requirements and identified the classes and the relationships among the different classes that use the system. There are three major analysis techniques used together during the object oriented analysis namely;

- **bject modeling:** This involves developing the static structure of the software system in terms of objects.
- **Dynamic modeling:** This examines the behavior of the system with respect to time and external changes after the static behavior of the system has been analyzed.
- **Functional modeling:**This shows the processes that are performed within an object and how the data changes as it moves between methods.

3.5.2 System Implementation

The buiding of the system started after having the design complete. this was done by writing code. The tasks were further divided among the different individuals working on the project. Each developer followed a predefined set of guidelines for collaboratin during the development process.

JavaScript and Solidity which is a language used to build smart contracts on the Ethereum platform, are some of the languages used. Another important software in this development is ganache. Ganache is a software that allows one to simulate a blockchain locally on a computer. Ganache has a number of features including displaying the accounts on the local blockchain, the transactions made, the blocks in the network, among others.

Finally, we use MetaMask to run the application on a browser. MetaMask is a google chrome extension that allows one run a blockchain application on google chrome browser.

3.6 Testing and Validation

3.6.1 System Testing

This phase involves the assessment of the system to verify if it works properly and also verify if it satisfies the specified requirements. The system has been availed to potential users to test it. This enables the team get feedback from the potential users of the system. There are two major approaches to testing of the system used ie;

- **White box testing:** In this technique, we critically studied the source code to find out which unit or chunk of code is behaving inappropriately. This helped in optimizing the code and removing extra lines of code which

bring in hidden defects or adding more lines of code to make the application work even better.

- **Black box testing:** in this technique, a tester interacts with the systems user interface by providing inputs and examining outputs without knowing how and where the inputs are worked upon.

3.6.2 Validation

Systems validation is the process of checking that a software system meets specification and it fulfills its intended purpose. To ensure data quality, errors should be detected during input, prior to processing and storage and this will be achieved through validating input transactions and input data. If the system conforms to the specified user requirements, the first release will finally be deployed. With time, the system will be upgraded with more improvements and innovative features; this is because systems without innovative features lose their usability in the long run.

3.7 Conclusion

To realize all this, we had to put into play our project management skills and this called for the need to track our progress using daily Stand Up meetings. This is recorded and shared on google sheets [6].

Chapter 4

System Analysis and Design

This chapter describes the study, analysis and design of the system. It highlights the identified requirements and Architectural design of the system.

4.1 Overview of the system

The system designed in this project is aimed at having students results stored and managed on a blockchain network. The management of the results on a blockchain network ensures more security compared to the traditional centralized systems.

The system uses Ethereum which is a platform that allows creation of blockchain networks. For this project, Ganache is used as the local blockchain network on a user computer. The user gains access to the network using browser extension known as MetaMask. Each transaction that involves adding something to the blockchain network costs a given amount of ether which is a currency used to transact on the Ethereum network.

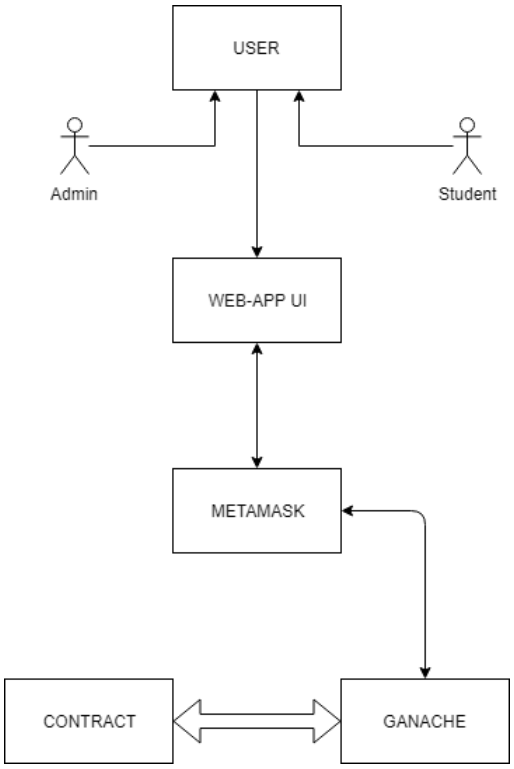

Figure 4.1: Simple system Architecture

4.2 System Analysis

4.2.1 Data Analysis

From the data retrieved during the research process, we found that the present system handling students records is prone to a number of errors and weaknesses.

The current system handling students results at Makerere University does not have a limit to the number of times a student can do a course as opposed to the actual policy by the University where a student is meant to sit for exams in a course not more than three times.

Another discovery from the data received was that the present-day system handling students results at Makerere University can accept an input of a percentage figure greater than 100%.

4.2.2 User Requirements

Below are the user requirements for the blockchain results handler.

- Allow an administrative assistant enter students results.
- Allow students to access their results without being able to change them.
- Allow employers gain access to job applicants' past academic results.

4.2.3 Functional Requirements

The functional requirements specify what the system is expected to do. These include the following;

- Provide verification of a user.
- Ensure that the students results are not altered.

4.2.4 Non Functional Requirements

The non-functional requirements describe the behavior of the system, and these include:

- The system must verify any addition to the blockchain.
- The system must notify the system administrator incase of any unauthorized transactions.

4.2.5 System Requirements

The system is built with a foundation on the ethereum network which is a platform that enables building of blockhain based smart contracts. MetaMask is a browser extension required for the system to allow a user access the ethereum blockchain network. All these have to be accessed on a Personal Computer with a browser e.g. google chrome, mozilla firefox among others.

4.3 System Design

This section includes a detailed description of the systems architecture, components, modules, interfaces, and data for a system to satisfy the specified requirements. It describes the design and development process of the application using a use case diagram to explain how the actors will interact with the system and data flow diagrams to show how data will move in and out of the system.

4.3.1 System Architecture

The system consists of the following major components:

- A blockchain network built on the Ethereum platform.
- A PC that is used to access the blockchain network.

- A user interface that allows a user to access the services of the system like adding to the chain, viewing results, among others.

Class Diagram

This is a static structure diagram that describes the structure of a system by showing the system's classes for example the student, Academic registrar, among others. It also shows their attributes, operations (or methods), and the relationships among objects.

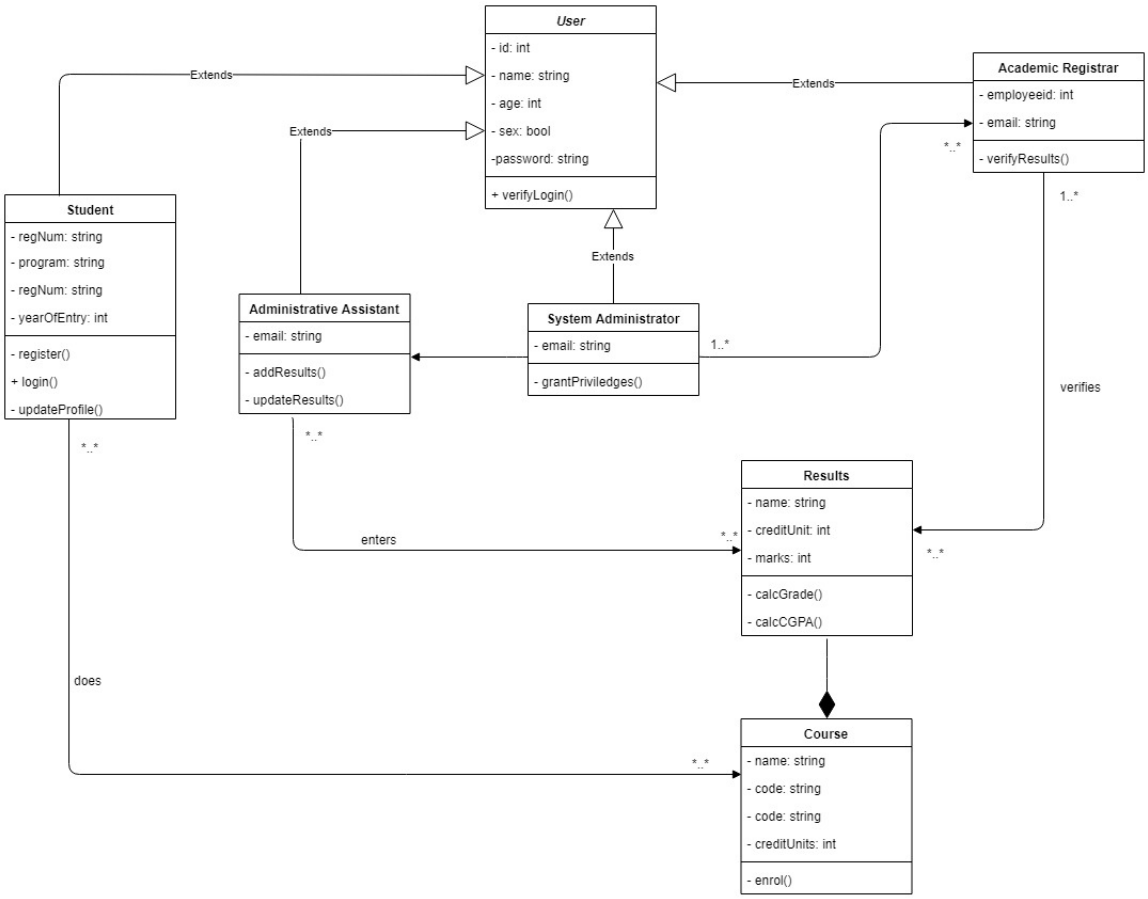

Figure 4.2: Class diagram

Use Case Diagram

This is a high level description of the different types of users of the system and how they interact with it. A use case diagram provides a simplified graphical representation of the systems functionalities.

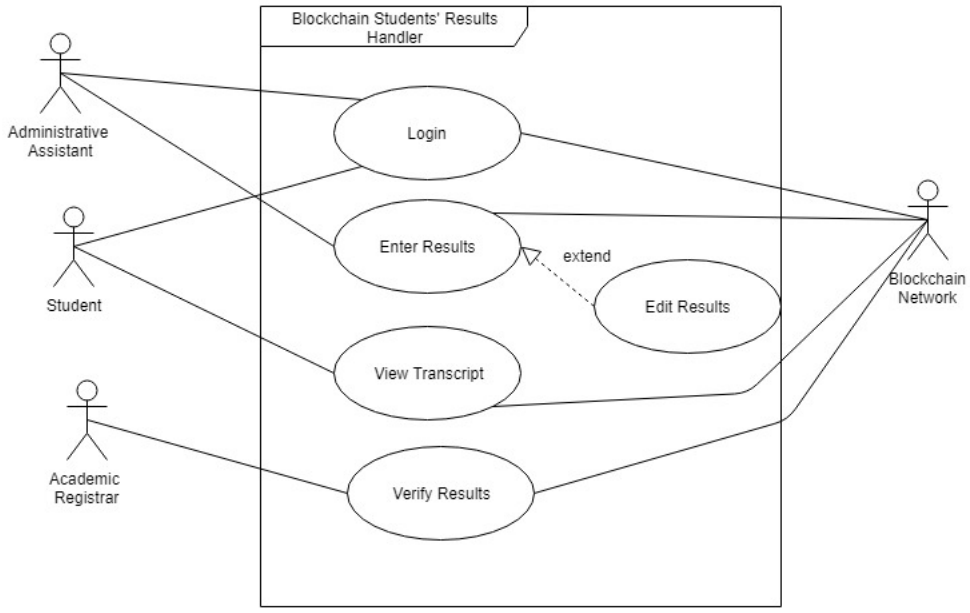

Figure 4.3: Use Case diagram

Context Diagram

This gives an overview of the entire system. In this diagram, there is only one process that represent the entire system. The purpose of this diagram is to display the expected inputs and outputs from the system to and from various entities. Shown in the diagram below is how various entities like students interact with the system.

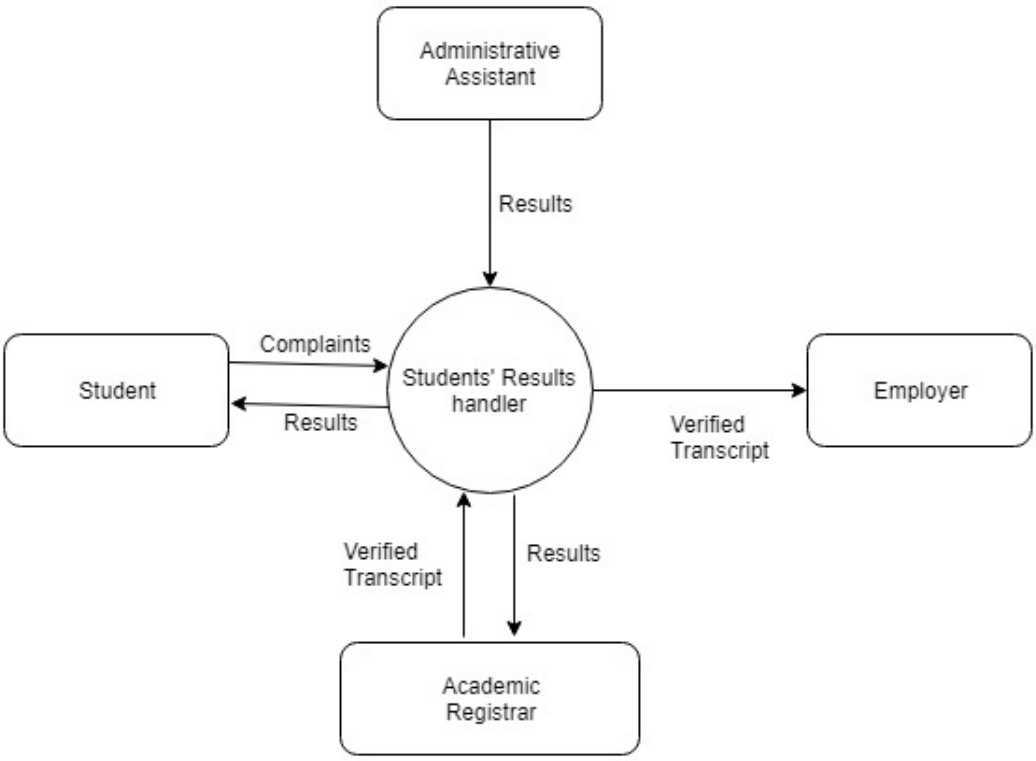

Figure 4.4: Context diagram

4.3.2 Design Constraints

Accessing the blockchain network requires reliable internet connectivity.

One needs to have the MetaMask browser extension installed on their browsers in order to access the blockchain network.

Writing to the blockchain costs gas. Gas in the context of Ethereum is a unit and a measurement for the computing power that is needed to execute certain

operations in the Ethereum Virtual Machine (EVM).

The developers were limited to only ten virtual accounts to simulate actual accounts during development.

Assumptions
Some assumptions were made during the design and development of the system which include;

The end-user is willing to learn and adopt to the technology that may be new to him/her.

Users always have good internet reception.

Users are familiar with common internet browsers and file extensions for these browsers.

Scalability of the system will not negatively affect the applications speed and reliability.

4.3.3 Design Methodology

We used the Agile software development (ASD) methodology. This methodology involves adaptive planning, evolutionary development, early delivery, and continual improvement. It also encourages rapid and flexible response to change. We focused on keeping code simple and testing often. This helped us to minimize risks such as bugs, cost overruns and the changing requirements.

4.3.4 Graphical User Interface (GUI) Design

This section provides the detailed design of the system and subsystem inputs and outputs relative to the user.

Inputs

Ethereum network password: the users password is required to create an account on the Ethereum network. If the user is logging in on a different device from a previous one that was used to access the network, theyll have to enter the seed phrase generated for them by the platform.

Results: When an administrative assistant logs into the system, he/she can enter the students results.

Outputs

Testimonial: before the results are forwarded to the blockchain, a student can access the system and view his/her progressive results.

Transcript: On accessing the platform, a student can view his transcript which can be printed as a pdf. An employer who would like to view an applicants past results can also access the network and view the same transcript.

4.3.5 External Interfaces

Hardware Interfaces

To fully access the functionality of this system, a user is required to have Computer with an internet browser(like google chrome, mozilla firefox, among others) with the MetaMask browser extension installed.

Software Interfaces

The functionalities of the external interfaces were developed using web-based scripting langauages like PHP, JavaScript and the blockchain network built on the ethereum platform.

Communication Interfaces

The student details handled by the system are stored on an online sql database. The fully processed and verified transcript is stored on the blockchain built on the ethereum platform.

User Interfaces

Users navigate through the application using a windowed GUI. This involves clicking using a mouse, dragging and dropping among other manoeuvres possible with a windowed GUI.

Bibliography

[1] Margaret Rouse, TechTarget(2018, September). *Cryptography*[article], Available: https://searchsecurity.techtarget.com/definition/cryptography

[2] Records Keeper(2018). *Verify Academic Certifications*[article], Available: https://www.recordskeeper.co/verify-academic-certifications/

[3] *The scourge of fake academic papers*[article], Available: https://www.monitor.co.ug/News/Education/jobs-dark-world-fake-academic-documents/688336-4784694-bvjkc7z/index.html

[4]]MyHub Team, (2016, June). *Intrant Security: How Secure Is Your Intranet?*[article], Available: https://www.myhubintranet.com/intranet-security/

[5] Luke Graham, CNBC News (2016, May). *Schools are using bitcoin technology to track students:*[article], Available: https://www.cnbc.com/2016/05/09/schools-are-recording-students-results-on-the-blockchain.html

[6] Donald Clark, OEB Global (2016, September. 12). *10 ways Blockchain could be used in education*[article], Available: https://oeb.global/oeb-insights/10-ways-blockchain-could-be-used-in-education

[7] *Google Sheets Daily Stand-Up Meeting Notes*[article], Available: https://docs.google.com/document/d/1eJhi8pN2b1Nc29sU-jxtM-PKZ6UtxqFijfrP1fr14F0/edit?usp=sharing

[8] Open Data Kit, ODK Community (2018). *The standard for mobile data collection*[article], Available: https://opendatakit.org/

[9] *Ethereum Project Blockchain platform to run smart contracts as they are coded to be*[article], Available: https://www.ethereum.org

[10] *Ganache A one click blockchain*[article], Available: https://truffleframework.com/ganache