ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 7, Issue 4, pp: (58-70), Month: October - December 2019, Available at: www.researchpublish.com

KENYA NATIONAL QUALIFICATIONS DEPOSITORY MANAGEMENT SYSTEM: A BLOCKCHAIN TECHNOLOGY APPROACH

FATMA KHAMIS ALI[1], DR. ELISHA O. OPIYO[2]

[1,2] SCHOOL OF COMPUTING AND INFORMATICS

[1,2] University of Nairobi

NAIROBI, KENYA

Abstract: **Globally, education is regarded as a stepping stone towards country's success and achievement of its goals. Academic qualification is considered as enough evidence of the possession of necessary skills and knowledge and a prerequisite for personal success in life. It is also viewed as an essential tool for establishment and progression of career which opens many opportunities in one's life. Due to this essential value attached to academic qualification, academic credentials as a symbol of academic qualification in Kenya and across the world are subject to falsification, forgery and other fraudulent means. Academic dishonesty may have been contributed by lack of decentralized qualification depository system for verification of authenticity of academic certificates in addition to the lack of realization of the benefits of Blockchain technology in this area. Studies revealed that in India such system was successfully installed to curb fake and forgery of academic certificates. Currently, there are methods, projects, and commercial systems present in the related domain, such as digital signature, eCert and Europass. However, they don't satisfy the verification requirements sufficiently due to their various design purposes. The objective was to design a trustable national depository system for managing certificates for Kenya National Qualifications Authority using a Blockchain technology approach, the research design is mainly quantitative involving the use of questionnaires and a few qualitative aspects from interviews which are to be filled by different stake holders and their response to be analyzed. The anticipated results of this study aimed to curb forgeries of academic certificates and scripts by building a system using a Blockchain technology that will provide permanent secured certificates and facilitate the process of verification of authenticity of certificates thus ease the accessibility by the stakeholders.**

Keywords: **Blockchain Technology, Kenya National Qualification Depository Management System**.

I. INTRODUCTION

Globally, education plays a vital role in empowering and stimulating country's economy and development growth as indicated by [1]. For any country to prosper has to empower its citizens with necessary skills and knowledge on different fields. Academic qualification is paramount to countries economic and development growth because it empowers manpower with necessary skills and knowledge for success and achievement of goals. Academic qualification is, therefore, considered as enough evidence of the possession of necessary skills and knowledge for one to succeed in many parts of the world. Academic credentials such as academic certificates and scripts are enough evidence for one to prove to be academically qualified in particular area. More often, academic qualification is considered by many as a prerequisite to personal success in life. It is also view as an essential tool for establishment and progressive career which opens many opportunities in one's life. In this light, is the wish of every citizen to possess minimum academic qualification necessary for securing employment opportunities, achievement of personal goals and success in life [2]. Nevertheless, due to fraud

which has become a menace in our society today particularly Kenyan society, forged academic credentials are everywhere across the country.

Forgery in our context may be defined as a process of adapting, making or replicating things such as documents or statistics with the aim of deceiving to make profit through selling such documents or alter the public perception. In addition, forgeries of documents and identity theft have been mentioned as the leading forms of fraud across the globe [3]. Moreover, fraud business of making forgery documents in backstreet has become a source of income for many fraudsters who capitalize on the need for everyone to have minimum qualifications for good life. Currently, academic certificates and scripts forgery has reached its heights in Kenya spearheaded by Kenyan street-wise fraudsters across the country. This has resulted into many unmerited allocations of positions and loss of engagements in government institutions and corporations in the country [4]. [5] indicated that, developing a secure digital system may resolve forgery and fake certificates. This study further revealed that in India such system was successfully installed to curb fake and forgery of academic certificates.

Academic dishonesty may have been contributed by poor academic policies in the country, over emphases on academic qualification or advanced technology advent. Since learners are the leaders of tomorrow of a country, their academic integrity and honesty are paramount aspect at the educational level. Currently, there are methods, projects, and commercial systems present in the related domain, such as digital signature, eCert and Europass. However, they don't satisfy the verification requirements sufficiently due to their various design purposes. In Kenya, to try and curb this menace, the government through the ministry of education proposed the introduction of Unique Personal Identifier (UPI) for all students in government schools from nursery school level to university level. UPI may be defined as a set of individually identifiable data which indicates a peculiar individual's identity and which may allow another person to access such information with personalized details. All students will be required to have the UPI connected with an electronic database. This will partly curb the menace of forgery but may not curb it fully. To solve the forgery of documents partly is a step towards total elimination but does not entirely solve the problem thus leaving a loophole for fraudsters to exploit [5].

II. PROBLEM STATEMENT

In the current economy that is hungry for jobs and skills, fraudulent matriculation certificates are on the rise, hence, necessity for pre-admission, pre-employment and on-going post-employment screening. According to statistics by Managed Integrity Evaluation (PTY) Limited, an international background screening company in South Africa, reveals that the number of matric certificates from world over that fail at verification process has risen from 21% in 2010 to 23% in 2012. In Africa, the percentage of misrepresented qualifications by candidates seeking employment or promotion stands at 31.83% and that for the rest of the world is 43.10%. A clear need for organizations to be more vigilant in checking qualifications of all their recruits, irrespective of their countries of origin [6].

Critical to an organization success, be it educational or business, is hiring talent with the right qualification, experience and skillsets. Whereas, the process of identifying the right talent ought to be smooth and efficient by use of certification and CVs presented by candidates at recruitment process, in this time and era of too many fake certificates, a further step for verification of whether paper or digital certificate is needed. This calls for either third parties to verify the certificate or the need for certification authorities to maintain a registry or database for certificates [6]

Fraudulent matric certificate due to lack of decentralized qualification depository for verification is, on one hand, a discouragement to qualified and hardworking candidates and loss of credibility of genuine institutions of learning [7]. On the other hand, the potential exposure for the organization to reputational and financial risks, losses, brand name are too high [6]. Hence the need for a system that can address secure data storage, decentralization and immutability. The Blockchain technology will provide solution as transcripts are recorded and distributed on a ledger to be easily accessible by individuals and other institutions locally and globally; the certificates cannot be altered since the distributed ledger is tamper proof; and finally saves money and is economical for both employers, students and other institutions as there is reliability and accessibility of the documents [8].

III. OBJECTIVES

The main goal of the proposed study is to develop a trusted software which will manage and verify academic qualifications for Kenya National Qualifications Authority using a blockchain technology approach.

Specifically, the study aims at:

a) Identify the current methods used to manage and secure certification process in institutions of higher learning

b) To identify how Blockchain technology can be used to offer transparency, secure, shareable and verifiable matric certification in Kenya

c) Design a Blockchain-based system for managing certification process in Kenya education system

d) Develop and evaluate the functionality of the Blockchain-based system

IV. FEATURES OF A SECURED SYSTEM OF EDUCATION CERTIFICATION

The objective of a system of certification is for certificates to be widely accepted by third parties through trust. [6] describes the methods and processes for trust creation in certification as follows:

Identity verification method

This method, using identity documents, verifies the parties involved in the transaction, both the issuer and the certificate holder. Identity documents, are themselves attesting to a person's identity.

Standardized processes for Issue and certification processes

As identity is key to trust, so is the methodology of making a claim by the issuer. Only after person meets certain set of criteria, that a certificate is issued. This requires that the methodology be documented in a standard, which is adhered to by all issuers. Noteworthy, is that in a system with multiple issuers, the higher the level of standardization in place across the network, so is the level of trust in that system

Regulation and quality assurance

In an established standardized system of certificates, trust that each of the parties in the system acts in good faith and applies those standards in line with their requirements is essential. In addition, the system should be able to expose, if need be remove parties that do not comply to enhance level of trust in the entire system.

Security features

A third-party wishing to verify the authenticity of a claim in a certificate must be able to ensure that such certificate is not forged. The two common ways to prevent such forgeries is through physical anti-forgery mechanisms such as signatures, watermarks, special designs incorporated into the certificate itself, which ensure that only the issuer could have made that specific certificate and through a database of issued claims, held either by the issuer or in a centralized database known as a registry, whereby a third-party can check that the claim has indeed been issued.

Accessibility

The final element for trust in a certificate is for the claim to be easily accessible. Accessibility implies that the recipient of the certificate should be able to hold a copy of the certificate; third parties who require access to the certificate should be granted access; the certificate should contain information as to how to verify the claim, and the standards and processes used to make the claim and issue the certificate; the information in the certificate should be clear, legible and easy to use.

V. BLOCKCHAIN IN EDUCATION

a) Blockcerts: An open Standard for Blockchain educational certificates

The cornerstone of the Blockcerts open standard is the belief that people should be able to possess and prove ownership of their important digital records. These records form the basis for proving aspects of oneself, consistent with the principles of self-sovereign identity ([9]. Within this context, the Blockchain is considered to be a technology that allows individuals to own their official records and share them with any third-party for instant verification, all the while precluding any attempt to tamper with or edit the records.

Blockcerts open standard for issuing and verifying credentials on the Bitcoin blockchain is an open standard platform for issuing and verifying records on the blockchain, and it is the goal of the Blockcerts community to promote its adoption as the main global standard (in terms of social adoption) for issuing records on the blockchain. The standard allows any

user, including education institutions and governments to use the base code and develop their own software for issuing and verification.

b) Gradubique: An Academic Transcript Database Using Blockchain Architecture

Gradubique is a blockchain network built on top of a Hyperledger fabric (HLF). Gradubique allows the posting of exams and course grades in the network, as well as give employers and graduate schools an opportunity to extract transcripts of an individual. In Gradubique, an academic institution submits a student's official transcript into the network where all the University for Example in USA will have to validate the transcript before it is added to the Blockchain. Thus the transcript is officially published in the Gradubique. Anytime the individual student wants to join a higher institution of learning or an employer wants to verify the document of the student, they can evaluate the transcript directly without the consultation of a third party.

Since Gradubique used HLF, which focuses on permission Blockchain network, members in the network are required to identify those who join the network as well as the organization as the certificate authority provider [8].

VI. PROPOSED CONCEPTUAL FRAMEWORK

The conceptual framework for the national academic depository is as illustrated below:

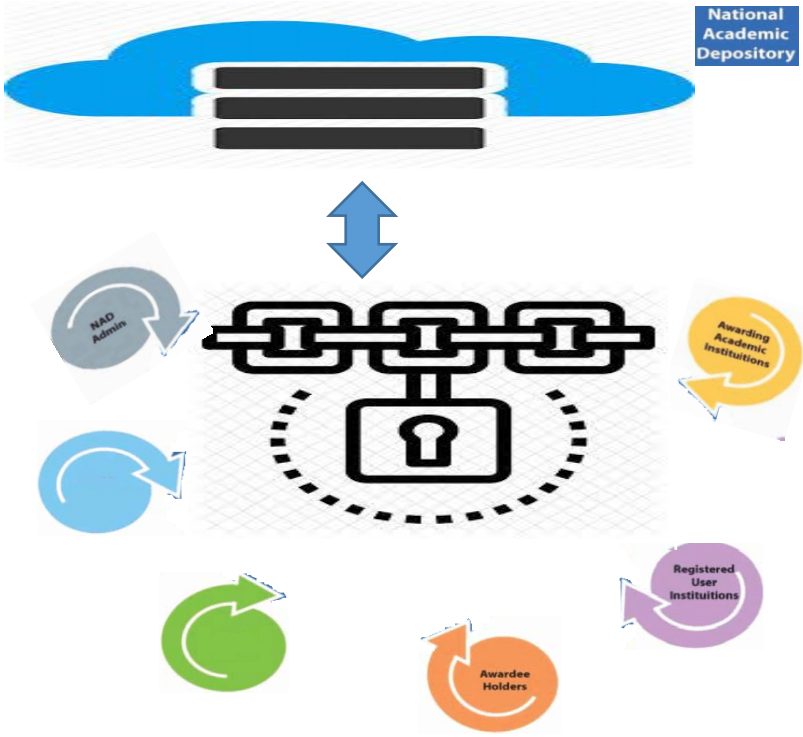

Figure I: Conceptual Framework

NAD will allow the logging of academic awards. In addition to ensuring the authenticity integrity, and confidentiality of the database, NAD can act as a deterrent to fake and forged paper certificates, reduce administrative efforts, and eliminate the need for institutions to preserve physical records.

Academic institutions are held responsible for the authenticity of NAD data. Requests for access to academic awards for potential employers require the consent of the recipient. Academic institutions include the following:

- Public Universities
- higher educational institutions and institutions Approved by the Government and ministry of education to grant degrees/diplomas
- Private universities
- CUE, KNEC, KASNEB and other boards

Other stakeholders include

- Students and other academic award holders
- Verifying entities e.g. banks, private companies, government entities, academic institutions
- Public Service Commission and HELB
- Depositories e.g. KNEC, KASNEB

Through the Blockchain technology all approved/valid users and stakeholders can submit/view certificate details in the national depository.

VII. METHODOLOGY

This section discusses how the research project was conducted. It looks at the research design and the system analysis and design and proceeds to the implementation.

A. Research Strategy

The concept of this research strategy comes from analysing the literature review that proved that the current management of national qualifications in education sector is not completely comprehensive, researchers focused only in part of how to make a secured and tamper proof system. There is a lack of the central depository for managing national qualifications to minimize if not completely eradicate forgery of academic credentials. The adopted research strategy presented the finding from analysing the previous studies in chapter two and supports the result by adopting case study from the real live, which is typically observing the characteristics of the research respondents, how they do their work. This is because the adopted strategy is proving the credibility results of analysing the previous studies.

Therefore, the research respondents were staff members at the Kenya National Qualification Authority who are charged with the management of all qualification from within and abroad. To be interviewed too were the academic registrars in selected public and private universities, and national examination bodies, because the staff members on daily basis use a certification management system in their routine. These people absolutely knew the limitation and /or problem in the current certificate management in the country. Conversely the students and employers may have suggestions which could help to enhance the quality national qualifications especially with the aim of all learning institutions who are targeting to deliver a very credible qualification. However, the reason of using such strategy was for achieving the problem statement of this research needs, which was to study and analyse the findings from the literature review and the current academic certifications system, which required the implementation of empirical research. So using a case study approach the researcher gained the drive to probe deeply into a national qualifications depository responses through interviewing the respondents at KNQA, universities and employment bureaus. The interview was conducted by asking the respondents several open questions, those questions are arranged in sequence starting with the current system effectiveness in the learning institutions and then the respondent's suggestions about the new system, then the respondent's answers were written as notes under each question asked.

B. System Analysis and Design

Object oriented analysis and design approach (OOAD) was used. According to [10] OOAD combines both processes and data into objects. This enables a better understanding of the problem and provides simplicity in transition to design phase [11]. Use case diagrams as well as verification flow diagram was used to help understand the functional requirements of the Qualification model to be translated into more detail plans for its implementation.

C. Evaluation of Prototype

Evaluation of prototype is considered the analysis of a given prototype that has been designed and later developed. Evaluation forms part of the methodology for this research. The evaluation of the prototype helped the research on getting the user performance views inform of feedback and also helped in looking at the performance of the prototype based on the objectives of the study. The research used an iterative process evaluation approach which consisted of five steps namely: confirm the prototype, develop questions, design methods, implement & adapt, and make decisions. According to [12], iterative framework guides innovators and evaluators in designing as well as evaluation of prototype. Figure II shows the iterative evaluation approach.

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 7, Issue 4, pp: (58-70), Month: October - December 2019, Available at: www.researchpublish.com

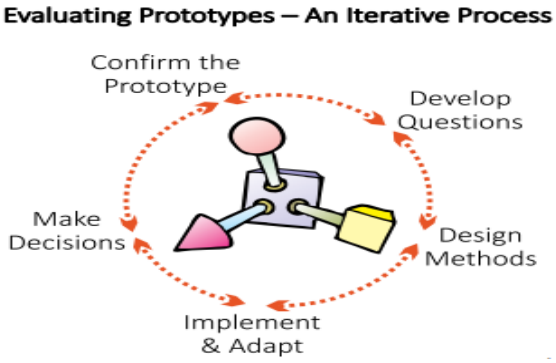

Figure II: Iterative approach of evaluation of prototypes [12]

D. Prototype Development

The qualification model was developed using the V-process methodology. This methodology offered a fast delivery of the system as it was broken down into modules thus allowed the researcher deliver a quality system since its main emphasis was on the verification and validation of the model at its early stages of development. It also allowed parallel development and testing of the system's deliverables

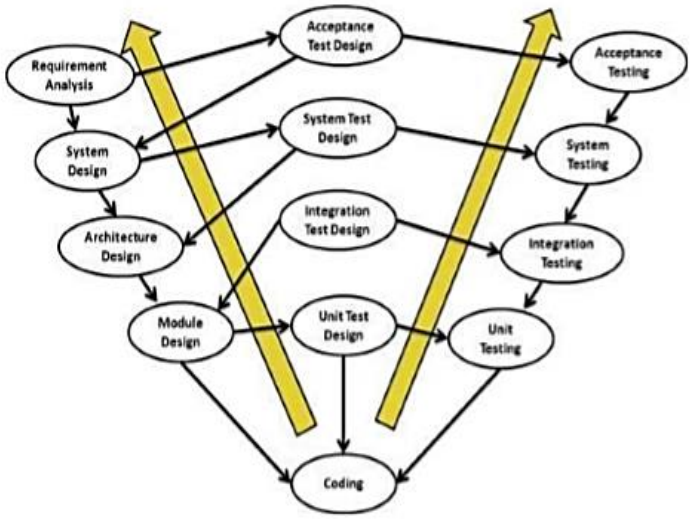

Figure III: V-process Model [13]

VIII. REQUIREMENT ANALYSIS

From analysis of the responses from the questionnaires administered, the study found out that there was a need of national qualification system that will ensure the certificates are secured and cannot be tampered with. This called for use of Blockchain technology to be implemented in designing the National academic qualification system. The system requirements can be explained as follows:

A. Functional Requirements

Functionality requirements includes all aspect of the system functions, basic operations, and the capabilities of the Qualification system. This entails process or activities like:

i. user management which gives the administrator the privileges to add, create, delete, account of a user.
ii. User request,
iii. sending notification,
iv. generation of reports,
v. updating information.
vi. Administrator, users, and institutions can all login and respond to a query.

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 7, Issue 4, pp: (58-70), Month: October - December 2019, Available at: www.researchpublish.com

B. Non-Functional Requirements

The non-functional requirements are the system qualities without them the system is considered to be functioning but their presence increases the instructiveness and make the system to user friendly. The non-functional requirements include the following:

i. security of the system which deals with authorized access since the system deals with very important documents
ii. how errors are reported by sending error logs to the system administrator to assist in trouble shooting of arising issues,
iii. system availability and reliability i.e a system that doesn't have costly errors and doesn't breakdown frequently,
iv. system responsiveness which the ability of a system to respond to a user request within the fastest time possible
v. system usability having a system it is easy to operate and learn.
vi. the system should be scalable making it easy to upgrade and customize cost effectively.

C. System Requirements

The Qualification system has a relation database management system which manages the central database. The central database stores and organizes data to facilitate manipulation. The system has a graphical user interface which provides a user friendly access point to the system. There is also security mechanism in place which is a password to ensure only authorized users can access the system. Finally, frequent backups will be done to prevent any case of loss of data should there be a system breakdown.

IX. DIAGRAMATIC REPRESENTATION OF THE MODEL

A. Use Case Diagram

The use case diagram described describes the user's interaction with the model. The use case diagram comprises of actors (system users) who in this study are the system administrator and KNQ, boundary which represents the limits to which the model operates and the use cases which are a collection of success or failure scenarios. The developed model has the following main actors: Admin (overall oversight of the system, manage valid Institutions and Employers), Institution (manages the overall student details (adds/ updates student's certificates, verifies, validates), Employer (query student certificates, verify certificate authenticity). Figure IV below shows the use case diagram of the KNQA system using Blockchain technology.

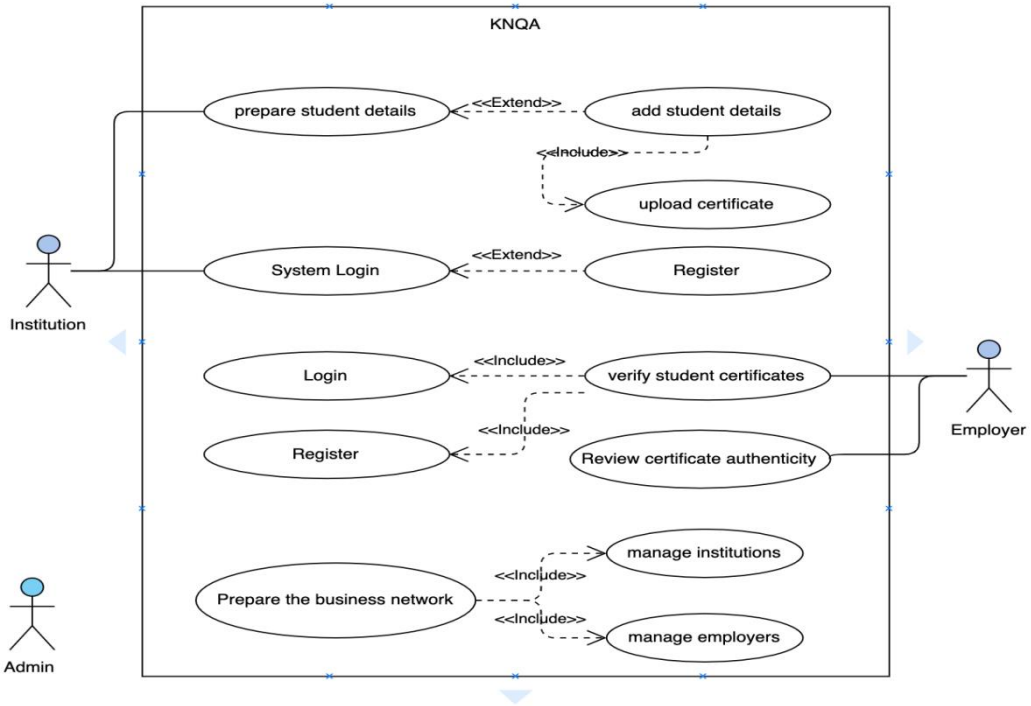

Figure IV: Use Case Diagram

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 7, Issue 4, pp: (58-70), Month: October - December 2019, Available at: www.researchpublish.com

B. Verification Flow

The main feature of this model is the provision of a system that enable verification of certificates through the national qualification system by employers, and institutions as well ensure that certificates submitted are genuine. Figure V shows the sequence of activities that are followed.

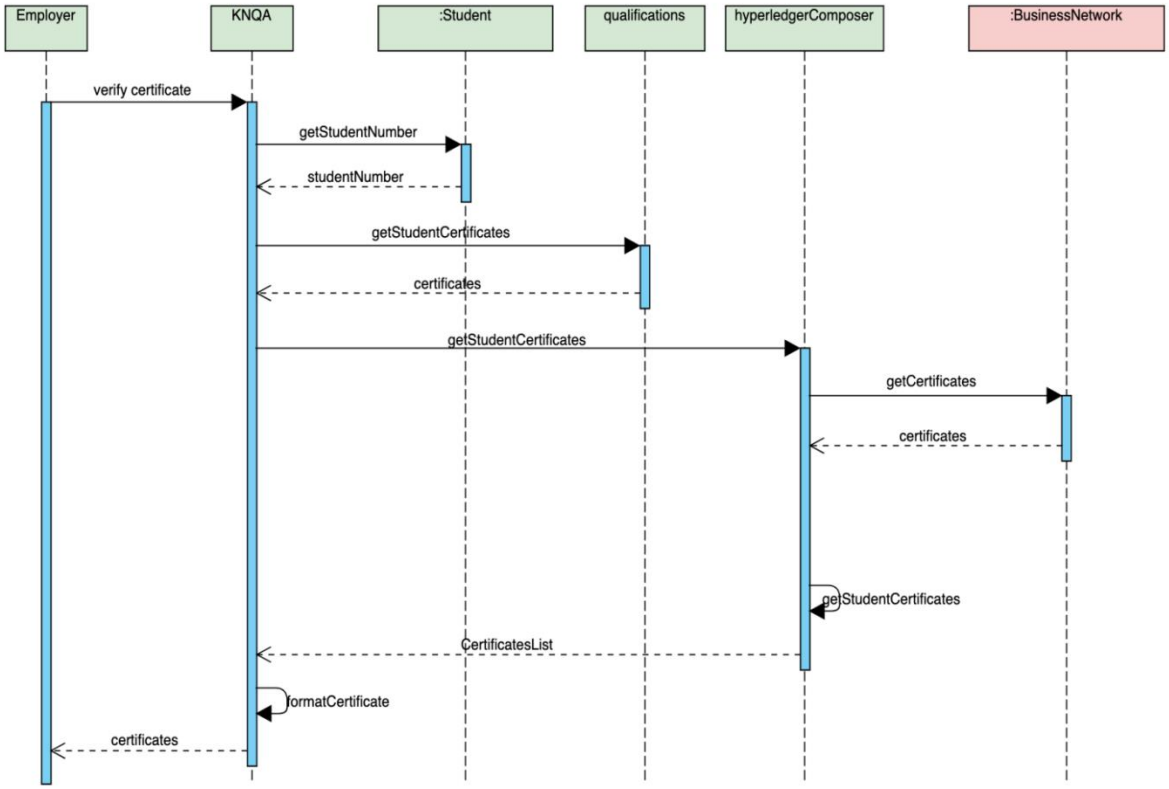

Figure VI: Verification Flow Diagram

C. Hyper ledger Composer MODEL RELATIONSHIP DIAGRAM

The model relationship diagram describes the model's data in terms of entities, attributes and relationships. All students, Institution and Employer are the participants of the business network. Institution has one to many relations with student, which translates to Institution can have many students. Students have one to many relationship with qualification where students can have many qualifications. Institutions can upload qualifications for specified student. On the other hand, Employers has one to many relationships to student qualification. Employers have access to many student qualifications. Students have several attributes which describe them. These include student Number, name, address(optional), institution, email(optional), phone(optional), the student Number is the unique identifier for student details. Figure VII below shows the entities for the KNQ model and how they interact with each other.

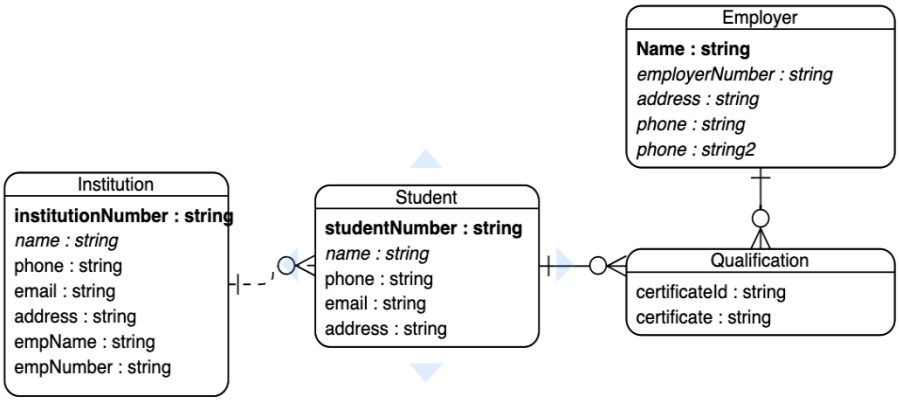

Figure VII: Composer Model Relationship Diagram

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 7, Issue 4, pp: (58-70), Month: October - December 2019, Available at: www.researchpublish.com

D. Design Hyperledger Composer Model

The diagram in Figure VIII provides a visual representation of the model interaction in the KNQA model, their attributes, their connections and associations. The system administrator can login, add one or more, modify or update institutions, students or update qualifications assets and log out. Also after logging in the system administrator (regulators) can view one to many reports. Academic institutions can login and add one or many students. Employers can login and search for students certificate data. Both the academic institution and employers inherit login and logout functions from the superclass "user".

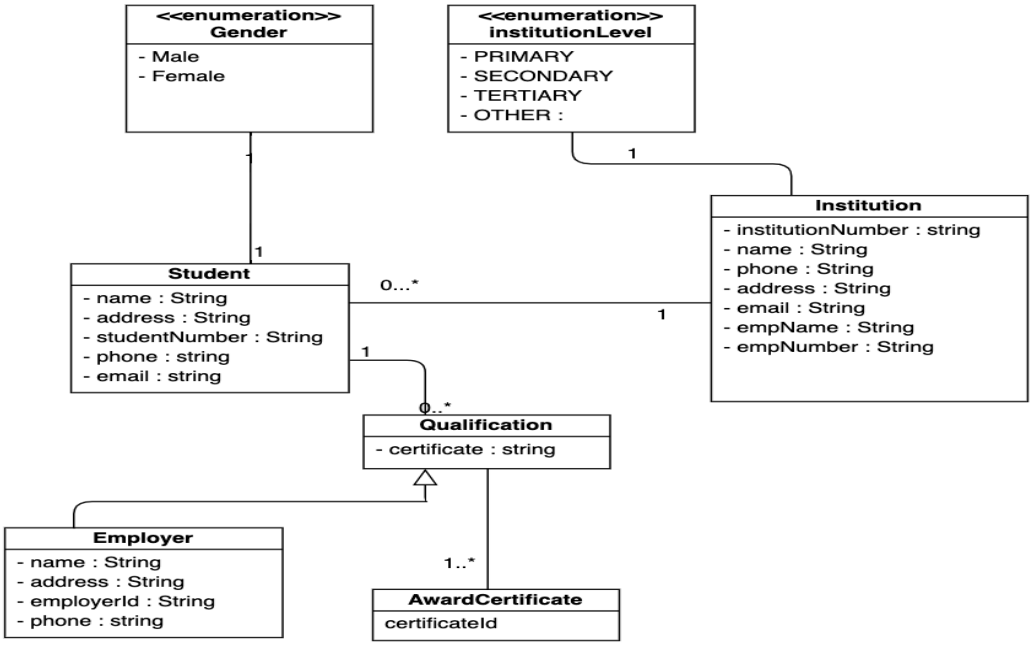

Figure VIII: Hyperledger Composer Model Diagram

X. SYSTEM DESIGN

A. System software interface

KNQA blockchain system is a client server application that is composed of different modules that will be accessed in the through a web client (i.e. browser). This section describes different main features for the KNQA blockchain system, whereby it provides a comprehensive architectural overview of the system, using a number of different architectural views to depict different aspects of the system.

B. System Hardware Architecture

The system is based on three tier architecture with the following components; the database, web server and the browser that lies on the client side. The browser on the client side lies on different computers or internet –enabled electronic gadgets.

The following hardware components are used in the system:

- Servers where web and application servers are hosted.
- Computers / internet-enabled electronic gadgets to access the system from the web

C. System Software Architecture

The KNQA blockchain network design is based on the individual design of various components in which users interact with the blockchain network. The following software components will be used:

- Hyperledger Composer - this is the environment on which the system will be built.
- Node.js(v8.16.1) – provides environment for running Angular applications.

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 7, Issue 4, pp: (58-70), Month: October - December 2019, Available at: www.researchpublish.com

- Node Package Manager(npm v6.4.1) - enables installations of extra node packages also essential in running of the client application.
- Web browser- e.g. Mozilla Firefox (v42.0 or later), Chrome (v42 or later)
- MongoDB – for managing system users
- Docker – managing system containers including Mongodb, composer rest server containers and the Hyperledger Composer environment.
- Angular (v6) – this is the framework client application is built on.

D. Hardware Detailed Design

The server should have the following requirements

- Ubuntu Linux OS (v16 or above) or OSX (v10 or above) – this is the required Operating Systems required for the Hyperledger Composer blockchain network to work correctly.
- Minimum 15 GB hard disk space
- 4 GB of RAM or above
- 2 GHZ CPU speed
- Network interface card
- USB port for connecting GSM modem
- RJ45 connectors to connect the server to the network.

E. Software Detailed Design

The system consists of the following modules. Each module is shown by a use case described in figure IX below having the specific functionalities.

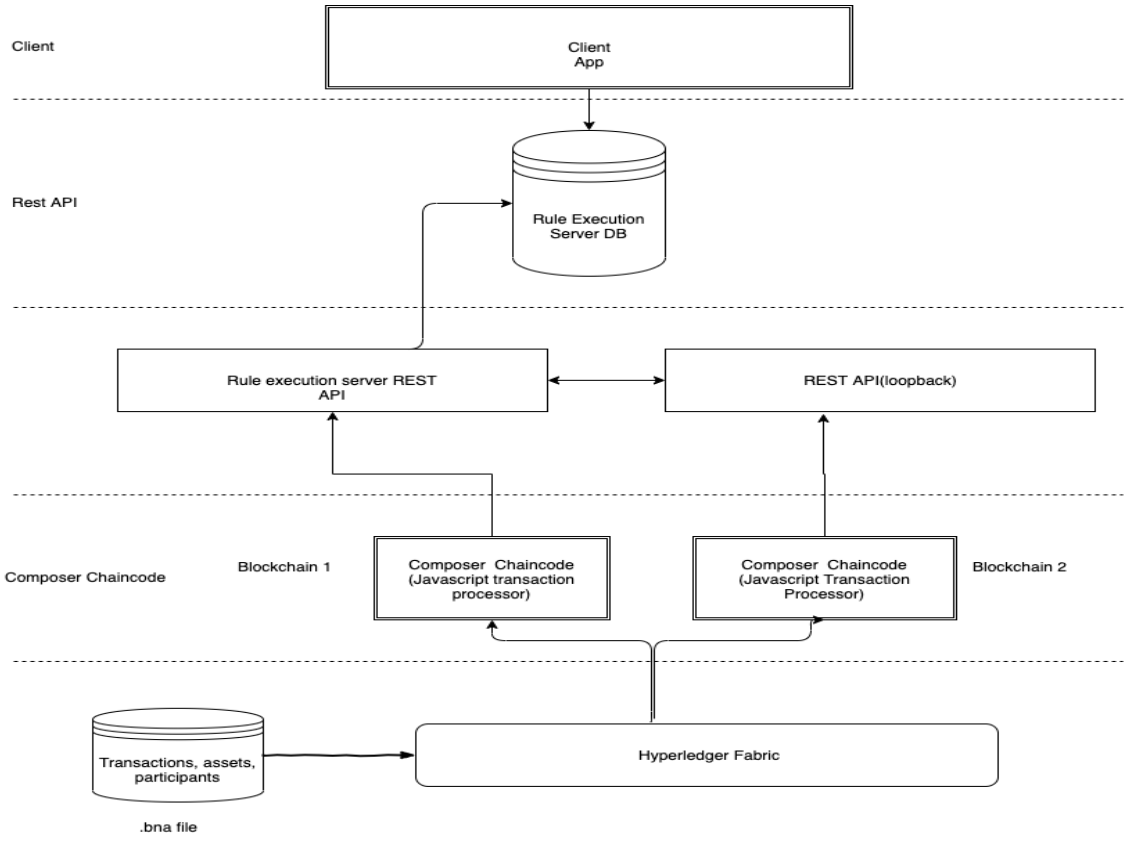

Figure IX: System Design

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 7, Issue 4, pp: (58-70), Month: October - December 2019, Available at: www.researchpublish.com

XI. SYSTEM IMPLEMENTATION AND TESTING

A. System Implementation

Angular 6 framework, JavaScript and Hyperledger Composer were used to develop the KNQA model. The Web interface (front-end subsystem) was developed using Angular 6 framework while the back-end subsystem was developed using Hyperledger composer. The front-end subsystem enables the users interact with the system and utilize its back-end capabilities. The back-end subsystem is comprised of the Composer rest server which helps system users interact with the KNQA business network logic. Back-end subsystem therefore receives data and responds to user's queries and requests. Angular was used because it is efficient, platform independent and intuitive framework for user experience.

B. Blockchain Technology In KNQA

Blockchain Technology in KNQA is build with JavaScript SDK which is split into:

- composer-client used to submit transactions to a business network or to perform Create, Read, Update, Delete operations on assets and participants.
- Composer-admin used to manage business networks (install, start, upgrade)

i. Composer Client

It provides the API that is used by business applications to connect to a business network to access assets, participants and submitting transactions. When in production this is only module that needs to be added as a direct dependency of the application.

ii. Composer-Admin

This module would usually be installed as a local dependency of administrative applications. This API permits the creation of and deployment of business network definitions.

iii. Rest Server

The Hyperledger Composer REST Server automatically generates an Open API (Swagger) REST API for a business network. The REST Server (based on LoopBack technology) converts the Composer model for a business network into an Open API definition, and at runtime implements Create, Read, Update and Delete support for assets and participants and allows transactions to be submitted for processing or retrieved.

iv. Transactions

Transaction reflects the business activity upon the business network. To achieve data immutability transactions are kept inside blocks and protected through a chained structure.

C. Model Testing

Several tests were done all through the model's development and implementation processes. These tests include: unit testing was done to eliminate bugs and ensure the modules functioned as expected, integration tests were conducted to verify that the modules built and tested independently can be integrated and can communicate and the system test to ensure that the functional and non-functional requirements of the model meet the user requirements and specifications provided. Usability test was also carried out to test the functionality of the collaborative model and to verify and validate that the communication components function as expected, the model easy to learn and use, the navigation flow is smooth and that the resultant system is user friendly and meets the user requirements and specifications.

D. Prototype Evaluation

The developed system was experimented by a number of users in order to evaluate its usefulness. The evaluation process was meant to check whether the system was working according to specifications and ensuring that both non-functional and functional requirements are satisfactory. The evaluation was done by the KNQA, KASNEB, University registrar (Umma University), and students (3). The aforementioned users were given the system to use it before there were given the questionnaire to confirm whether the requirements were met. The evaluation aimed at achieving the following objectives:

1) To ascertain the presence of a working prototype (availability).

2) To check the ability of the system to offer transparency, secure, shareable and verifiable certification (effectiveness).

3) To confirm if the system is user friendly.

Evaluation Results of the Prototype.

Following the evaluation of the system by four users totaling six in number, the following was the findings:

a) There was a general consensus that a system for verifying academic certificates was present and working. Thus the system was acceptable and working and did not have any signs of runtime errors during execution.

b) The system was found to be user friendly by 66.7% (4) of the users, however 33.3% (2) felt that the user interface still needs some working especial in aesthetic perceptive i.e. beautification of login page with a background that is appealing and symbolic to academics. Generally, users agree that the system was easy to use and learn.

c) In relation to appropriateness of the system, the users unanimously agreed that the system was appropriate and timely in dealing with the issues of fake certificates in the market. However, 50% of the users (3) were skeptical on whether the system security will be easily breached, since they had little knowledge of Blockchain security.

d) The users (6) unanimously agreed that the system will look complete if additional features are included like transcripts and photo of the certificate holder to provide full identification and details.

XII. CONCLUSION AND RECOMMENDATION

A. Achievements

The following were achievement as per the study objectives:

1) The main goal of the proposed study was to develop a trusted software which will manage and verify academic qualifications for Kenya National Qualifications Authority using a Blockchain technology approach.

2) Identified how Blockchain technology can be used to offer transparency, secure, shareable and verifiable matric certification in Kenya.

3) Designed a Blockchain-based system for managing certification process in Kenya education system.

4) Developed and evaluated the functionality of the Blockchain-based system.

B. Findings

Based on the data collected, there was a need to have verification of academic certification that cannot be tampered with once entered. The various institutions studied showed there was a need of such a system. The study also showed the willingness and ability of these institutions in adapting Blockchain technology for verification of certificates.

C. Challenges and limitation

The use of Blockchain technology in Kenya is still in its infancy and has not been fully adopted in Kenya.

D. Recommendations

Based on experience from the study, the following recommendations were made:

1) Blockchain technology awareness should be done to help people understand the technology and its advantages and also help clear away the illusions and misconception about the technology.

2) Academic institutions and recruiting agencies should make use of the KNQ system to help them verify the authenticity of documents that pass by them.

3) Another research model should be carried out to help improve the KNQ prototype.

E. Conclusion

Blockchain technology is trending globally, with bitcoin as the major application. However, the concept is still new and confusing to many but it's only a matter of time that people will understand the advantages of Blockchain technology and

its application should be all over especially as we gear to achieving our vision 2030 goals. It is my hope that the prototype will be useful in dealing with issues of certificates verifications and validation, and the prototype is open to any improvement to help solve the problem of fake certificates especially in Kenya where such cases are alarming.

REFERENCES

[1] Mason, R.O., (2017). Four ethical issues of the information age. In Computer Ethics (pp. 41-48). Routledge.

[2] Gupta, S. and Sadoghi, M., (2018). Blockchain Transaction Processing; springer International Publishing

[3] H. Ferradi, R. Geraud, D. Naccache, and A. Tria, (2015) "When Organized Crime Applies Academic Results." IACR Cryptology ePrint Archive, p. 20.

[4] Géraud, R. (2017). Advances in public-key cryptology and computer exploitation. Cryptography andSecurity , PSL Research University

[5] Gupta, V. (2013). A National Academic Depository. European Scientific Journal, ESJ, 9(19).

[6] Grech, A. and Camilleri, A.F. (2017). Blockchain in education.

[7] Muthoni, J. M. (2015). E-verification. A case of academic testimonials. Masters Thesis, University of Nairobi, School of computing and informatics.

[8] Nguyen, T. (2018). Gradubique: An Academic Transcript Database using BLOCKCHAIN Architecture. Requirements for CS 298, San Jose State University , Department of Computer Science .

[9] Allen, D. (2017). Discovering and developing the Blockchain crypto economy.

[10] Russell, S., & Norvig, P. (2013). Artificial Intelligence: A Modern Approach (3rd ed.). London: Prentice Hall.Hoffer, J. (2001). Modern Systems Analysis and Design.

[11] Hoffer, J. (2001). Modern Systems Analysis and Design.

[12] Cabaj, M (nd). Evaluating Prototypes. Aid4Action, Retrieved on 30th June 2019 from https://www.tamarackcommunity.ca/hubfs/Resources/Tools/Aid4Action%20Evaluating%20Prototypes%20Mark%20Cabaj

[13] Khan, P. M., & Beg, M. M. (2013). Extended Decision Support Matrix for Selection of SDLC-Models on Traditional and Agile Software Development Projects. Third International Conference on Advanced Computing & Communication Technologies, (pp. 8-14). New Delhi.