International Journal of Computer Applications Technology and Research
Volume 11–Issue 07, 255-263, 2022, ISSN:-2319–8656
DOI:10.7753/IJCATR1107.1002

A Blockchain-Based Conceptual Model for Curbing Institutional Academic Certificate Fraud

Esther Kabibi Nzaro
Institute of Computing and Informatics
Technical University of Mombasa
Mombasa-Kenya

Kennedy Ondimu
Institute of Computing and Informatics
Technical University of Mombasa
Mombasa-Kenya

Fullgence Mwakondo
Institute of Computing and Informatics
Technical University of Mombasa
Mombasa-Kenya

Abstract: There is need of certificate authentication mechanism in Africa, specifically in Kenya that will solve internal fraud activities. This is because there are many fake certificates in circulation that appear to be genuine but were obtained illegal from accredited universities. This is caused by the assumption that certificates being issued at the university are authentic. While authentication of the final academic certificate has been studied in previous research, many researchers focused on securing the final academic certificate and assumed that all certificates issued by universities are genuine thus creating a loophole for institutional certificate fraud. It's possible for clients looking to get an academic certificate illegally to collude with university staff, who are responsible for generating the certificates, to acquire a legitimate academic certificate without going through the academic process.

The purpose of this research is to develop a blockchain based model that solves the current problem of institutional certificate fraud. The research targets only Kenya public universities. Sampling will be done using simple random sampling to identify a few universities that will participate in the study. A combination of secondary data and primary data will be used in the research. Secondary data will be used to test the model while primary data will be used to construct the data mapping structure/model. Primary Data will be collected from the registry department using questionnaires and interviews while the sample will be obtained using stratified sampling. The model will be deployed using permissioned blockchain. The proposed model will have controls to ensure a student goes through the entire learning process before he is awarded an academic certificate.

Keywords: Certificate authentication, blockchain, accreditation, certificate fraud, internal fraud

1. INTRODUCTION

In the world over, academic certificates are used in many places including universities and job places as a way of confirming one having acquired some specific skill set. It is therefore a norm to be asked to produce the credentials as a proof of one's claim of having completed a course. The relevancy of certificates comes into play while seeking to further studies, job employment, job promotions etc. In Kenya, for example, legislation required all members of parliament and governors have a degree. This led to many politicians who were not graduates and needed to vie for elective seats seek for the certificates. Academic certificate authentication has become equally important now days as a way of validating the different credentials acquired from different learning institutions.

Due to the significance attached to the academic certificates, an increase in different kinds of academic certificate fraud has been witnessed. Academic certificate fraud is the deliberate effort to use fake credentials knowingly and deceive people for personal gain. Academic certificate fraud is a threat to the intellectual integrity in which knowledge advancement depends on. Consequences of academic certificate fraud range from personal reputation, organizational reputation, the integrity of the institutions and effects on the economy and also could be fatal, for instance, a fake surgeon who operates people using a fake certificate. Academic certificate fraud taints the reputation of the institutions and its honest scholars and researchers. It may also cause investors to the institutions withdraw their support due to lack of integrity. Another negative impact is that people with fake certificate may be given jobs at the expense of those individuals with legitimate documents. Wrong job placements result into poor performance causing employers to suffer great losses. This may cause great harm even to students who legally acquired certificates from same institutions since no one will trust them. Individuals may also face the law against certificate fraud once the certificate have been proved beyond doubt to be fake. These malpractices cause even great harm in some critical domains like medicine, aviation, military etc. Some of the implicated cases include doctors, nurses and pilots etc. In 2013, the global corruption report on education recorded corruption instances exceeding a global average of seventy percent. One of the reasons that has contributed to the increase of certificate fraud is employers over relying on the academic certificates for employment and promotions at work places. This has made many workers to look for more academic certificates using all means at their disposal. In Uganda, the government in 2016 investigated Busoga University for giving over 1000 fake degrees to south Sudanese students who needed to secure government jobs back in their homeland [1]. In 2017, Uganda arrested 88 members of staff at Makerere University who colluded with students by altering students' grades and issuing of fake degrees [2].

Academic certificate fraud exists in many forms depending on the techniques used. Most common techniques used include manipulation of academic documents, bribery of university staff to forge academic certificates, bribery to ensure the licensing of academic institutions, ghost schools only existing on paper, the passing of examinations, fake admission into education programs and the award of degrees [3]. As a result, academic certificate fraud can be classified into document fraud, institutional fraud, diploma mills and accreditation fraud [1]. Some of these activities are easy to

detect but some very difficult to detect if advanced mechanism is not used. From research that has been done to curb the occurrence of certificate fraud in institutions, much focus has been the final academic certificate verification and authentication. The emerging problem is internal fraud where an employee may be bribed to manipulate records in the official university document so as to help someone get a certificate while he never attended any class or attended class but has never met all minimum requirements. The certificate may pass all verification and validation process since it is supported by the university official documents. To address the gap of institutional fraud, a solution is needed that will prevent internal staff of a university in charge of certificates from controlling when certificates are generated and for who. Controls need to be implemented right from the admission of students and keep track on the entire learning process. Blockchain technology is ideal for the proposed model to solve the current problems and loopholes in the certification process because of its desirable features such as transparency, elimination of trust on people and the immutability of records. This paper introduces a novel blockchain-based model for curbing institutional academic certificate fraud. By using blockchain in this model, we utilize its intrinsic features like immutability, decentralization, enhanced security and distributed ledger. The proposed model will make it impossible for learning institutions to admit students who do not qualify in their courses of choice, get an academic certificate before the lapse of the course duration and alter exam results stored in the blockchain. By preventing the three above, the model will thus prevent any form of certificate fraud thus ensuring that verified academic certificates are authentic. In addition, smart contracts will eliminate the trust placed on the people working in the certificate sections as they will not have control on who to generate certificate for. Certificates will be generated based on the certificate information from smart contracts, which is automatically fired once a student meets the requirements for certification. This therefore means that certificates generated out of the certificate information from smart contracts will fail the validation test during certificate verification using the blockchain.

The following is the main contributions of this work in summary:

i) This research proposes a unified data mapping structure that can be adopted by any university to allow it store data in the blockchain.

ii) By using blockchain, this model allows for distributed storage of academic certificates which is therefore tamper-proof, void of cheating and fraud.

iii) Strong cryptography of blockchain ensures that data stored in the blockchain has high degree of security and privacy even as it can be accessed by any third parties e.g. employers

2. PRELIMINARIES AND RELATED WORKS

2.1 Blockchain Technology

Blockchain technology is a distributed database that records transactions in a distributed ledger. Blockchain is a combination of many techniques such as cryptography, mathematics, algorithms and distributed consensus algorithms. It's characterized by features that makes it to be used in different domains for trust free systems.

Blockchain was first used to a peer-to-peer ledger for record keeping of the transactions of Bitcoin cryptocurrency. A blockchain transaction in the public ledger contains a verifiable record and once the information entered, it cannot be altered or erased in the future. The Blockchain technology eliminates third-party intermediary and allows for verification of transactions directly [4] Transactions completed are made available to all participating nodes thus becoming more transparent than the centralized database. Once consensus is met by all nodes, the record is added to the block. Each block contains a hash value of its last counterpart for connection to other blocks to form a blockchain [5]. Blockchain technology is being used in certificate authentication because it eliminates the need of trusted third parties. It has many desirable characteristics that gives it an advantage to other technologies. These desirable features include decentralized, immutability, timestamp, trust and transparent as described below [6]

1) **Transparent**: Blocks of transactions are made available to all participating nodes thus promoting transparency of transactions. It's also very difficult to rollback or delete a transaction once it is added to the blockchain. Blocks with incorrect transactions are quickly identified and cannot be added to the blockchain.

2) **Decentralization**: Blockchain is a distributed ledger where all transactions are shared to all participating nodes in the blockchain. This ensures that data is available even with a failure of participating node. It eliminates the problem of centralized database where when the relied source fails then all transactions and services fail. It also eliminates the problem of relying on third party agencies for some services such as verification and authentication of transactions.

3) **Immutability**: Blockchain is a technology that makes it difficult to change a record once it is added to the blockchain. This makes records to be tamper proof thus retaining originality of the transactions.

4) **Authenticity**: Blockchain ensures authenticity because of the decentralized system, the blockchain data is complete, consistent, timely, accurate, and widely available.

5) **Trust**: Another feature of blockchain is trust. This is because the technology eliminates the need of third party agencies to ensure integrity of transactions. Each block is verified independently by consensus models which provide rules for validation of the blocks. Once consensus is made by the different nodes, the block is added to the blockchain.

Figure 1 shows the different features of blockchain.

International Journal of Computer Applications Technology and Research
Volume 11–Issue 07, 255-263, 2022, ISSN:-2319–8656
DOI:10.7753/IJCATR1107.1002

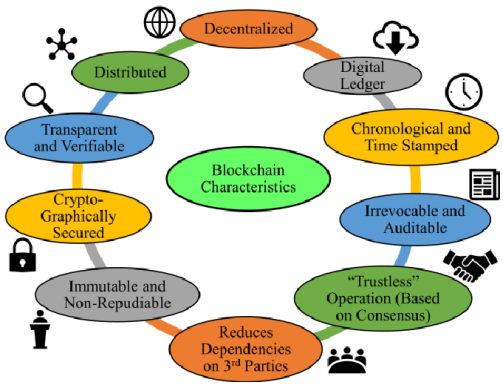

Fig. 1. Features of blockchain

There are three types of blockchain namely private blockchain, public blockchain and consortium blockchain. In public blockchain, information is open to the public and anyone can join the network and access information. It is a permission less type of blockchain. Private blockchain are permissioned. Only authorized individual who are approved can join the network and access information. Permissioned blockchain architecture ensures strict separation of roles and privileges. This makes it easy for system audit. Even if one participating node is honest, it will detect any malicious practices [1]. Consortium blockchain is a type of blockchain that is management by more than one organization. It's permissioned but some data could be accessible to the general public. It's more secure because participating nodes are geographical spaced [6]

Blockchain working begins when a node initiates a process and signs it with its private key, a block presenting the transaction is created on the platform. The transaction is broadcast to the peers within the network. The peer nodes then validate the transaction, after validation, it included in the block. At this point the transaction is confirmed. The block gets added to the ledger and links itself to the previous block. When a new block arrives after it, it cryptographically links itself to the back of the block. Figure 2 below shows the architecture of blockchain.

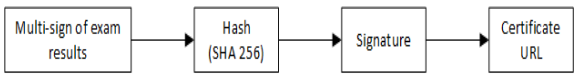

Fig. 2. Blockchain architecture

At the heart of blockchain is smart contracts. Smart contracts are programs stored on a blockchain that automatically execute when predetermined conditions are met. They are used to automate the execution of an agreement so that all participants can be immediately certain of the outcome, without any intermediary's involvement or time loss. Smart contracts are one of most attractive features associated with blockchain technology [7]. Smart contracts have various applications such as services in the financial domain, market prediction, utilization of the Internet of Things (IoT) [9], [10]. In the government sector, there are several smart contract frameworks and applications such as e-government, digital rights management, social media platforms, cloud storage, supply chain, smart transportation. This technology is used together with blockchain technology as the underlying technology to achieve trust less decentralized systems. Blockchain has a multi-signature wallet that can be used to collaboratively sign a transaction. Multi signature wallet is a well-known concept in the public cryptographic. It allows multiple parties to jointly sign on a document using their private keys. This practice is common where parties need to be in agreement for a transaction to take place [11].

2.2 Theoretical Framework

Theoretical review explains existing theories that are relevant to the study. This study is founded on fraud triangle theory and technology acceptance model theory.

1) **Fraud triangle theory**: Fraud triangle theory developed by Cressy in 1953 discovered three reasons why an employee may decide to commit fraud. The three elements are Pressure, opportunity and rationalization. Opportunity on the other hand is a weakness in an organization system that presents a chance for an employee with powers to commit and hide fraud. On the, other hand, rationalization is a personal justification of doing fraud in the organization. Instances of rationalization is "am doing it because others are doing it" or revenge to his bosses. Last but not least is pressure. It is either an external force or internal force or a threat making you to commit fraud [12]. The relevance of fraud triangle to the study is that institutional certificate fraud is done by employees of the organization and not people outside the organization. The three reasons stated by Cressy why employees may commit internal fraud positively relate to what may ignite an employer assist someone get a legitimate certificate without going through the learning process and meet minimum requirements to be awarded a certificate. A weak control system poses a greater opportunity to employees to commit and hide crime. On the other hand, it could be an Order from senior person to do a fraudulent act or an employee may do it because of personal interest. [13] Argued out that Opportunity carries a big risk to internal fraud cases compared to rationalization and pressure. He states that strong control systems and policies will eliminate any opportunity posed to employees to conduct crime even if under pressure or for his personal interests The theory supports the research on why there is need to develop a model to curb institutional academic certificate fraud by ensuring strong control system to eliminate any chance or opportunity posed to employees to commit fraud. In the existing certificate authentication systems, there exist opportunities (system loopholes) that internal employees may exploit and conduct certificate fraud. This is because existing solutions do not cover the process before the certificate 4 is generated creating an opportunity for internal fraud. These opportunities include but not limited to changing the enrolment date

and date of completion to suit client demand, falsify a record of non-existing student, illegal register a student in a program he doesn't qualify to, change grade to improve performance of a student, change classification of student, create fake transcripts for non-student etc.

2) **Technology acceptance model theory**: The theory was developed by Davis in 1985.Technology acceptance model theory is a theory majorly used in information systems. It specifies two components that determine the acceptance of technology by users. These elements are perceived ease of use and perceived usefulness of technology [14]. Prior to Davis work, Slevin and Schultz in 1975 carried out research and found that perceived usefulness of technology gave a reliable prediction of use of technology. [15] Replicated the work of slevin and Schultz and confirmed that there is a high correlation between perceived usefulness of technology and technology usage or acceptance [15]. Technology usefulness to the subject under research is a determinant of the usage and adoption of the technology and solution developed. This theory is relevant to the research on how to curb institutional certificate fraud since the solution proposed acceptance will depend on the relevance and usefulness of the technology used to build the solution. In this research blockchain technology will be used to develop the proposed model due to its usefulness and relevance of the technology to the problem under research. Blockchain technology abilities such as decentralized, transparent, tamper proof, immutable, timestamp preserves the state of document which creates integrity of the digital asset and makes blockchain more useful and ideal to certificate authentication than other technologies.

2.3 Types of Certificate Fraud

The malpractices in education sector can be classified into several ways such as document fraud, accreditation bodies' fraud, fabricated documents, diploma mills and institutional fraud [1].

1) **Document fraud**: Document fraud are falsified documents that are as a result of altering legitimate certificates or fabricating the entire documents by using fake logos, seals and serial numbers. [16] gave an example of document fraud where the Syrian migrants and refugees were sold forged documents on their way to Europe at the Syrian-Turkish border. Another fraud related to this is Accreditation bodies' fraud where accreditation bodies get compromised and legitimize false documents. The federal investigation agency in Pakistan probed many instances where regulatory bodies approve false degrees of powerful people [8].

2) **Diploma mills**: This is where fictitious universities sell fake credentials. Diploma mills operate in a highly structured and sophisticated manner that they make their customers have trust in them as legitimate universities. A recent example is the Axat international scandal where a Pakistan based company has a web of more than 370 diploma mills which collectively earned millions of dollars as revenue by selling fake degrees for various fictitious universities to clients worldwide [17]

3) **Institutional fraud**: Institutional fraud is where someone colludes with the relevant university employees to conduct fraud. A student or non-student of a particular university may bribe the employee so as to append his record in the university official document and get a certificate. A good example of this type of fraud is in the case Makerere University in Uganda where 88 members of staff were sacked for colluding with students to change their grades and issuance of fraudulently degrees. A similar case is the Busoga University in Uganda that awarded over 1000 tuition premium degrees in one month to south Sudanese in 2016 most of them being military so as to secure jobs in their homeland. This type of fraud is difficult to detect since it's backed up by the university records and it can withstand many tests imposed by accreditation bodies [18]. In Kenya for instance, it was found out that a few of current civil servants have fake degree papers and some still searching for papers in preparation for next year's election.

2.4 Academic Certificate Authentication Techniques

There are several ways that different institutions use to authenticate certificates both manual and automated solutions. The certificates are verified to check their validity through various means which include calling the said university to ascertain the certificate, by use of the accreditation bodies to verify certificate, use of Security holograms and institution seals, Verified university lists, Certified true copies, Verification forms/confidential letters, while technology based solutions include use of digital signature, use of Quick Response codes, use of blockchain technology and use of web application systems.

1) **Manual authentication**: This is done by an organization contacting the institutions in which the certificate originates so that they can validate a credential of interest. The institutions do manually verification at a given fee and it takes a lot of time since they have to go to archives and retrieve files in order to verify the certificate. This type of verification is also based on trust of the involved employees. In case these employees are compromised, they may end up validating an illegal certificate [19]. Other forms of manual authentication include security holograms and institution seals, verified university lists, certified true copies and verification forms or confidential letters written to employees.

2) **Technology-based techniques**: This is where the verification process in online and automatic i.e. it does not require human intervention.

Quick response code: A Quick response (QR) code is a machine-readable code consisting of an array of black and white squares, typically used for storing information for reading by the camera on a smartphone. QR codes

have been widely used to store information and can easily be scanned by mobile devices. A study done by [20] used QR code and digital signature to authenticate secondary school certificates so as to easy certificate verification process. It is a known fact that QR-codes can be exploited and easily be created over the internet. However, few studies have shown that QR codes can be secured with traditional security methods such as encryption thus QR codes cannot be used independently. This study didn't address the institutional fraud problem at hand since it cannot be used to record the learning process of the students so as to eliminate internal fraud.

Digital signature: Digital signature is a mathematical technique used to authenticate a digital document [21]. It involves the use of a pair of keys i.e. private and public keys and the hashing function. Private Key is used to encrypt the document while the public key is used to decrypt it. Digital signature checks for the integrity of information in transit between the sender and the receiver. Key may be hacked or lost which poses a security threat. Considering the problem at hand, digital signature cannot be used independently to control the learning process of students hence cannot be used independently to solve the problem of internal fraud.

Blockchain technology: Blockchain has been previously used in the academic sector to provide solutions to the forged certificate problem due to its characteristics. Characteristics such as time stamp, permanent, immutable, transparent, authenticity, decentralized makes blockchain an ideal technology to be used for certificate authentication and validation.

2.5 Related Works and Research Gap

2.5.1 Related Works: There are a number of existing solutions developed using blockchain technology such as blockCert, smartCert and EduCTX and frameworks that could be adopted in the certification verification

The initial research done by knowledge media institute (KMI) of the Open University (OU) initiated the use of badges and using ethereum to turn badges into smart contracts. KMI developed a prototype for issuing micro-credentials in the blockchain. In this research, certificate verification by other parties other than the insurer was not put into consideration. Similar research with same objective was done by [5] who developed a decentralized digital certificate application based on blockchain. This technology was selected because of its desirable features such as incorruptible, secure and permanent. The researcher needed to solve the problem of security where only physical documents were presented for verification in different events such as registration for courses, during interviews etc. Physical certificate led to mass duplication and alteration of certificates since it was difficult to verify with decentralized digital certificate application. With the use of digital blockchain based application, different institutions could verify the authenticity of certificate hence minimizing the problem of forged certificate. A similar initiative done by [22] is the open standard named blockCert that is used to develop apps for authenticating academic credentials. Certificate stored in the blockchain cannot be altered but BlockCerts is based on the self-sovereign identity of all the participants by providing components to create, issue, view and verify certificates in the blockchain. One of the drawbacks is, it does not have a separate validation service for verifying its validity. It also does not address some fraud cases such as the internal fraud.

[23]

Did a research on Security analysis of a blockchain-based protocol for the certification of academic credentials and found out that the blockCert standard lacks a way of verifying the ownership of keys used in signing of issued certificates as mentioned above. This may lead to impersonation of the insurer profile. The research proposed the use of public key infrastructure (PKI) to solve the problem. Another research done by [24] employed digital signatures and timestamps using blockchain technology. With the use of timestamp it made it difficult for one to claim having graduated earlier because records in blockchain cannot be changed thus reducing document fraud to a bigger extent. The researcher spells out that if the fraud takes place the same day of graduation, then it would be difficult to detect since the record will appear to be legitimate in blockchain thus still providing space for internal fraud.

A certificate verification framework using hyper- ledger to address security concerns such as confidentiality of information, authorization, ownership and authentication was developed by [25] Hyper-ledger was selected because of its desirable features such as permissioned access, transparent network and Uniquely Identifiable Digital Certificate SmartCert is another blockchain platform for credential verification and authentication. SmartCert was developed to establish the authenticity of academic credentials on a blockchain and to overcome the problem of fake certificates. SmartCert makes use of cryptography signing of educational certificates to provide transparency in the case of recruitment. The certificate holder shares the hash with the prospective employer to verify the certificate [25]. Again this solution does not address the problem of internal fraud and an illegal certificate that originated from the university will be approved as authentic. Another problem is the complexity of keys. The complexity of keeping and maintaining a series of keys triggered research on usability by [1]. The research focused on certificate verification and how they can tailor their solution to the existing verification ecosystem. Their main focus was on usability since many proposed solutions were not usable because parties have to maintain series of keys for authentication and authorization. They designed and implemented an online solution "Cerberus" one just need to scan the QR code to authenticate the certificate while maintaining all security features.

EduCTX is another research done by [26] was based on the concept of the European Credit Transfer and Accumulation System (ECTS). They proposed a blockchain-based higher education credit platform which exploit the benefits of the blockchain, as a decentralized architecture, offering security, anonymity, longevity, integrity, transparency and immutability. The goal of the research was to unify higher learning institutions systems so as one can access his or her credits scores from any university in case of transfer of students from one country to another. The EduCTX platform is implemented on the blockchain platform ethereum on a consortium-based network of Ethereum run nodes. The platform enables a globally efficient, simplified and ubiquitous environment to avoid language and administrative barriers [27].

2.5.2 Research gap: There is significant research on academic certificate authentication however researchers assumed that certificates issued by universities are genuine. Solutions

discussed above focused on the final certificate verification and not the entirely certification process. There is still lack of controls in the process leading to acquisition and issuing of the academic certificates. They make an assumption that certificate originating from a legitimate university are genuine thus covering internal fraud. It is possible for clients looking to get an academic certificate to collude with university staff, who are responsible for generating the certificates, to acquire a legitimate academic certificate without going through the entire academic process. Some of the activities that university staff may do which leads to internal fraud include

- Append a record of a fake certificate into the blockchain system so that it can be verified as genuine.
- Change students details like date of enrolment, date of completion, grade obtained in the local database so as to validate a counterfeit certificate.
- Accessing the local database and change grades.
- Classifying students in higher ranks which they do not deserve.

Due to the above reasons, a solution is needed that will eliminate all the loopholes that may lead to certificate fraud especially by internal staff of a university. Controls need to be implemented right from the registration of students and keep track on the learning process. Blockchain technology is ideal for the proposed model to solve the current problems and loopholes in the certification process because of its desirable features such as transparency and elimination of trust on people and the immutability of records.

The learning process of students' controls can be categorized into admission of student controls, examination in the entire program controls and finally issuance of an authentic certificate. It's evident from previous research that admission and examination has not been considered in the existing models but tackled final certificate authentication. This creates the loophole of internal fraud. Variables in student admission and examination needs to be captured into the blockchain and stored in the blockchain. This is because once information is stored in the blockchain, it is difficult to change since blockchain is distributed and makes it difficult for an individual to change. This brings in transparency and immutability of blockchain technology.

To avoid internal staff conducting fraud, conditions in the blockchain has to be set to ensure students meet and go through the entire learning process. In the proposed model, this is achieved through smart contracts. Smart contracts are self-executing programs that execute once conditions are met. In the proposed model, the variable defines smart contracts (program structure, progression smart contract and certificate smart contract), student details, Student Exam score and graduation date need to be captured into the model at different levels or times during the learning process and certification.

3. PROPOSED SOLUTION

3.1 Blockchain

Decentralization is one of the salient features of blockchain, which means that no single party or authority is governing or looking after the blockchain network. Parties make transaction through consensus thus establishing trust in a trustless network where there is no middleman involved. Another salient feature is a public ledger which ensures that every transaction is recorded in blocks. For a transaction to be accepted, every party needs to verify its validity. If majority of the parties agree that it's valid it is added to the public ledger. Once a record is added to the public ledger, no one can edit or delete the record. This promotes transparency and makes the entire process to be corruption-proof. Cryptography, another key intrinsic feature of blockchain is responsible for the security of records in the blockchain network [28]. By using blockchain in our solution, the entire certificate acquisition process is stored as transactions in the blockchain public distributed ledger thus making the academic certificate information to be secure, authentic and verifiable.

3.2 Academic Certificate Block

The academic certificate information will be stored in the blockchain to make it accessible on request and also authenticate the certificate. The process consists of four main components as follows:

i. Designated signatories use multi-sign to record exam results in the blockchain. Recorded exam results must conform to the established data mapping structure.

ii. Just like bitcoin, our solution uses SHA 256 in implementing the hash function during storage of the results. Any record added to a block in this models blockchain will consist of a hash of the actual exam result, a signature by the owner (student) and a URL to the stored results in IPFS.

iii. All academic certificates generated will be signed by the owner (student) any access to the record will require authorization from the owner.

iv. A URL to the academic certificate information for every academic certificate will be stored in the blockchain to make it possible to access the credential upon approval by the owner. Figure 3 shows the process of recording exam results and how the certificates will be stored in a controlled manner.

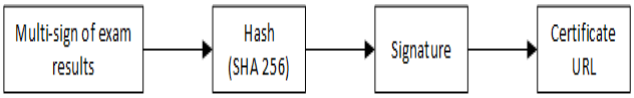

Fig. 3. High Level blockchain transaction for academic certificates

The details of each block in the academic certificates blockchain is as shown in figure 4 below.

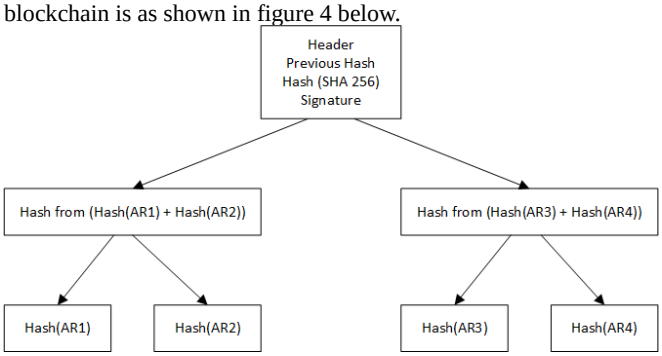

Fig. 4. Storage of academic records in the blockchain

The header contains the hash of the previous block, the hash of data to be stored plus the signature. AR1, AR2, AR3 and AR4 denotes Academic Record 1, Academic Record 2, Academic Record 3 and Academic Record 4 respectively.

3.3 Conceptual Model

Model Architecture: The detailed conceptual model synchronizes interrelated components and variables which help in solving a real-world problem. It clearly shows how components, variables interact with the process so as to eliminate internal academic fraud. Below is a model clearly showing the variables and the steps involved so as to eliminate internal academic certificate fraud? Figure 5 shows the conceptual model.

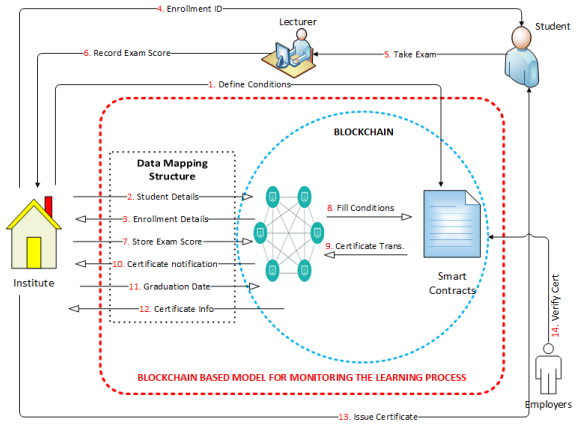

Fig. 5. Detailed conceptual model

Description of the conceptual model: It outlines the description of the process flow which takes into consideration all the requirements before admission of students, admission and examination activities and finally issuance of certificates.

a) **Define conditions:** These are smart contracts which are self-executing once the conditions are met. Three smart contracts will be defined by the learning institution which serves as a guide for the admission process, examination process and generation of academic certificates. The three smart contracts defined by the learning institution are as follows

1) **Course requirement smart contract**: The course requirements for admission will be defined for each academic programme. Here the overall minimum required and subject-wise minimum requirements to be admitted to a particular programme will be specified.

2) **Progression smart contract:** The programme structure for a given programme alongside criteria for progression to the next level of study is specified. Once a student successfully meets the requirements for the current level study i.e. after passing all required exams, the progression smart contract will elevate the student to the next semester and/or year of study. This will continue up to the final year of study, after which the student will be eligible to get a certificate.

3) **Certificate smart contract**: On completion of a programme duration and exams marks for the entire period having been filled, a certificate transaction or notification is generated. The institution provides additionally information such as the date of graduation to the blockchain. Classification is done inside the blockchain and information for preparation of a certificate is sent to the institution so as to prepare a physical certificate for the student.

b) **Admit student**: On admission, the student details and performance of the student is entered into the system. An API fills the course requirement smart contract to check with the pre-defined conditions for the particular course.

c) **Enrollment details**: The blockchain generates student enrolment Id if the student meets the course requirements.

d) **Issue student enrolment**: ID The student will be issued an ID using the information from the course requirements smart contract.

e) **Take Exam**: At the end of the semester, students will take exams for the units that they had registered for in that semester.

f) **Record Exam Score**: After students take their exams, lecturers mark the exams and records the scores for each student in the university system.

g) **Store Exam Score**: Exams undergo normal processing as per the requirements of the institution. Once results are declared, they are then added to the blockchain using multi-sign.

h) **Fill Conditions**: Each score of a student will be filled in the progression smart contract which executes once all the marks for a given semester are received. This continues until such a time when all the marks for a particular course are captured then the certificate smart contract gets executed. This initiates the process of generation of the academic certificate.

i) **Certificate transaction**: Once a student completes all the course requirements, passes all the required exams, the certificate smart contract is triggered. Upon execution, the certificate smart contract generates a certificate transaction.

j) **Certificate notification**: Once the certificate transaction is processed, a notification is sent to the institute to provide additional information such as date of graduation.

k) **Graduation date**. The graduation date is sent to the blockchain by the institute.

l) **Certificate information**: Certificate details are sent to the institution for purposes of generation of the certificates.

m) **Issue certificate**: Based on the certificate information, a certificate is printed and issued to the student. Also, multi-sign of the exams officer and registrar academics is required to be able to generate the certificate. The certificate contains the student details, classification, graduation date, issuance date and Code. The code can be used later to verify the authenticity of the academic certificate.

n) **Verify certificate**: Anybody can verify the authenticity of an academic certificate by use of code embedded on the academic certificate. On successful authentication of the certificate, you should see the student details, classification, university, date of graduation and issuance.

3) How the Proposed Model will Curb Internal Certificate Fraud:

- Admission of students is controlled since the student ID comes from the blockchain once the admission

conditions are met. This therefore makes it impossible to assist in admitting students who do not qualify.

- Performance of students for each unit in a semester is written in the university system. Once the results are declared, they are then saved into blockchain using multi-sign. The results thus become immutable, transparent and verifiable. This ensures that internal staff cannot change grades to assist students or disadvantage some students.
- Multi-sign of the departmental exams officer, chair of department and the chief exams officer is used to write students exam score. This spreads the risk of corruption since to insert a new falsified record requires collaboration of the three signing officers.
- Once all conditions have been met, the student will now be eligible to be awarded a certificate and the certificate smart contract gets triggered. After the certificate has been processed, the certificate information is stored in the blockchain using multi-sign of the relevant authorities. Once information is stored in the blockchain, it becomes permanent and very difficult to change.

Certificate information that did not originate from the blockchain cannot be appended into the blockchain thus unverifiable. This process limits internal staff who can be bribed to generate fake certificates and append them to the blockchain so that they can be verified as genuine but are not, therefore the model takes care of all loopholes used in internal certificate fraud..

4. VALUE OF THE PROPOSED SOLUTION

4.1 Benefits to Universities

The proposed solution will help universities to strengthen and seal all loopholes that internal staff can use to conduct internal certificate fraud. This will enable authenticity of academic certificates originating from universities. The article will help higher learning institutions to maintain their integrity and reputation. By eliminating institutional academic certificate fraud which taints the reputation of institutions, institutions will be able to attract more investors and researches to the institutions.

4.2 Benefit to Employers

On the other hand employers will benefit from the research in that they will be able to employ the right people for the right job which will automatically reflect in higher performance and productivity. It will also be easy for employers to verify certificates

4.3 Benefit to Students

Adoption of this model will mean that students are guaranteed of acquiring genuine certificates which can be authenticated by third parties.

5. CONCLUSIONS

By incorporating the salient features of blockchain, our solution will enable educational institutions to issue authentic and verifiable academic certificates thus curbing the gap of institutional fraud which is the hardest to prevent and detect. This will in a great way increase the reputation of educational institutions consequently increasing the quality of education as a whole. These academic certificates will be stored in the blockchain thus it is accessible on request by other educational institutions and employers. The students will approve any request for academic certificate verification in order to maintain data security and privacy.

6. REFERENCES

1. A. Tariq, H. B. Haq, and S. T. Ali, “Cerberus: A blockchain-based accreditation and degree verification system,” arXiv preprint arXiv: 1912.06812, 2019.

2. S. Trines, “Academic Fraud, Corruption, and Implications for Credential Assessment,” World Education News+ Reviews, World Education Services, 2017.

3. G. Sweeney, Global corruption report: Education. Routledge, 2013.

4. P. Bhaskar, C. K. Tiwari, and A. Joshi, “Blockchain in education management: present and future applications,” Interactive Technology and Smart Education, 2020.

5. J.-C. Cheng, N.-Y. Lee, C. Chi, and Y.-H. Chen, “Blockchain and smart contract for digital certificate,” in 2018 IEEE international conference on applied system invention (ICASI), 2018, pp. 1046–1051.

6. Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, “An overview of blockchain technology: Architecture, consensus, and future trends,” in 2017 IEEE international congress on big data (BigData congress), 2017, pp. 557–564.

7. A. Kosba, A. Miller, E. Shi, Z. Wen, and C. Papamanthou, “Hawk: The blockchain model of cryptography and privacy-preserving smart contracts,” in 2016 IEEE symposium on security and privacy (SP), 2016, pp. 839–858.

8. E. S. Negara, A. N. Hidayanto, R. Andryani, and R. Syaputra, “Survey of Smart Contract Framework and Its Application,” Information, vol. 12, no. 7, p. 257, 2021.

9. G. Wood and others, “Ethereum: A secure decentralised generalized transaction ledger,” Ethereum project yellow paper, vol. 151, no. 2014, pp. 1–32, 2014.

10. S. K. Hafizul Islam, M. Sabzinejad Farash, G. P. Biswas, M. Khurram Khan, and M. S. Obaidat, “A pairing-free certificate less digital multisignature scheme using elliptic curve cryptography,” International Journal of Computer Mathematics, vol. 94, no. 1, pp. 39–55, 2017.

11. D. R. Cressey, “Other people’s money; a study of the social psychology of embezzlement.” 1953.

12. M. J. Hopper and C. M. Pornelli, “Deterring and Detecting Financial Reporting Fraud; A platform for action, (October), 55.” 2010.

13. F. D. Davis, “A technology acceptance model for empirically testing new end-user information systems: Theory and results,” Massachusetts Institute of Technology, 1985.

14. D. Robey, “User attitudes and management information system use,” Academy of management Journal, vol. 22, no. 3, pp. 527–538, 1979.

15. Diana Jean Schemo, “Web boosts sales of bogus diplomas,” https://www.montereyherald.com/, Jun. 29, 2008.

16. M. Hasan, A. Zaib, H. Alam, and Z. Ahmad, “Blockchain Enabled Degree Verification for Pakistani Universities,” Pakistan Journal of Computer and Information Systems, vol. 3, no. 2, pp. 23–39, 2018.

17. Ezell, “How to Identify Diploma Mills and Axact Websites, and Tools for Your Protection,” College and University, vol. 95, no. 1, pp. 47–56, 2020.

18. M. Kirya, “Corruption in universities: Paths to integrity in the higher education subsector,” U4 Anti-corruption resource centre. U4 Issue, no. 10, 2019.

19. J. A. Otuya, “A blockchain approach for detecting counterfeit academic certificates in Kenya,” Strathmore University, 2019.

20. B. Shibwabo and R. M. Kaibiru, “A Prototype for authentication of secondary school certificates: a case of Kenya certificate of secondary education,” 2017.

21. M. Rouse, “Digital signature,” Search Security. TechTarget, 2014.

22. M. Jirgensons and J. Kapenieks, “Blockchain and the future of digital learning credential assessment and management.” Journal of teacher education for sustainability, vol. 20, no. 1, pp. 145–156, 2018.

23. M. Baldi, F. Chiaraluce, M. Kodra, and L. Spalazzi, “Security analysis of a blockchain-based protocol for the certification of academic credentials,” arXiv preprint arXiv:1910.04622, 2019.

24. F. Bond, F. Amati, and G. Blousson, “Blockchain, academic verification use case,” Buenos Aires, 2015.

25. O. S. Saleh, O. Ghazali, and M. E. Rana, “Blockchain based framework for educational certificates verification,” in Studies, Planning and Follow-up Directorate, Ministry of Higher Education and Scientific Research, Baghdad, Iraq. School~…, 2020.

26. M. Turkanović, M. Hölbl, K. Košič, M. Heričko, and A. Kamišalić, “EduCTX: A blockchain-based higher education credit platform,” IEEE access, vol. 6, pp. 5112–5127, 2018.

27. M. Hölbl, A. Kamisalić, M. Turkanović, M. Kompara, B. Podgorelec, and M. Heričko, “EduCTX: an ecosystem for managing digital micro-credentials,” in 2018 28th EAEEIE Annual Conference (EAEEIE), 2018, pp. 1–9.

28. K. Christidis and M. Devetsikiotis, “Blockchains and smart contracts for the internet of things,” IEEE Access, vol. 4, pp. 2292–2303, 2016.