Table of Contents

List of Figures

List of Tables

ABSTRACT

Verification of degree is a challenging task; one has to send degree to the respective university to get the verification of any candidate. It also takes lots of time. However, the new technology namely blockchain, is introduced which provides a secure way to store transactions in distributed ledger. It can resolve the degree issuing and transcript mechanism. The key benefit of using this technology is to verification will be easy and faster.

Degree Verification System aims to develop a digital degree verification system using blockchain technology. This will help to maintain the record and issue a digital copy of degree to the user. The System will be a web-based system consists of two module. One will be for university admin & endorsers whose responsibility will be to enter and endorse the data of students. Another module will be for those who will verify the originality of degree provided by enrollment id of student.

The report will look into features of system, tools & technologies and project methodologies that will be used to implement the working prototype of a system. The system will use the Hyperledger Fabric Blockchain Framework, Golang for smartcontracts(chaincodes), Nodejs for webservices (APIs) & Angular/React for web frontend. Also, the docker containerization will be used to deploy blockchain network & smart contract in the local system.

Introduction

Degree and transcript play an important role in the life of students in many ways like finding a job or getting admission for higher education. These academic credentials like degree, certificates or transcript issued by the academic institutions. Authorities manage their records manually or semi-manually and there is not any secure way to verify whether the document is real or fake. Also, in all over the world, there are many cases has been registered regarding to fake degrees. Verification of degree is also a challenging task; one has to send degree to the respective university to get the verification of any candidate. It also takes lots of time. However, the new technology namely blockchain, is introduced which provides a secure way to store transactions in distributed ledger. It can resolve the degree issuing and transcript mechanism. The key benefit of using this technology is to verification will be easy and faster.

This will help to maintain the record and issue a digital copy of degree certificate to the user. This will facilitate degree issuer to issue degree at that end of completion of the program it also increases security, reliability and efficiency. It will facilitate to Viewers (e.g. IT employee) to verify the originality of degree. This will also be beneficial for increasing reliability, detecting fraud, reducing cost & time, and lifetime record keeping.

Literature Review

Nowadays educational institutions are facing a very serious problem if fake degrees it is growing concern of many governments and hiring agencies. People and some fake degree mafia are running it as business in order to earn money and to help corrupt government official to get their way into politics and earn a seat in high table of government just to do corruption, this one side of picture to lower level people buy fake degrees to get hired by to rating agencies and to get high paid jobs.

There is this big fraud of fake degrees is present around the officers of human resources department and the managers of companies which there to hire employee they need to be very vigilant. This is called scam of fake degrees. These degrees are just generated from fraud organizations, in process of obtaining them no class work was done neither any assignment. Therefore the person who is carrying this kind of scammed degrees they don't actually have the required qualification mentioned in that degree.

The organizations which are involved in fake degrees business they just print a large number of these fake degrees for almost every profession a person can imagine. If a person has money then he/she can get whatever degree they want in whatever field of their choice without attending any lecture at any university or taking any exams. Any person with intelligence can crack this is a big problem. It is clear that no employers want to hire a person carrying fraud degrees which are actually not qualified for the job. It degrades the company's efficiency and overall its reputation [1].

According to General Medical Council it's the duty the employers of to check for fake or real qualifications of their employee in addition to medical degrees. Head of higher education degree data check told that only twenty percent of United Kingdom hiring officials go through the proper degree verification of their employees. He also said that while during all this buying fake educational degree was not illegal in United Kingdom. But one way to punish a person legally was using misrepresentation of employment constituted fraud this will lead ten years in imprisonment.

Medical governing board are true in sense that doctors are allowed to do their practice in medicine if they have real degree. The head of NHS told that NHS believe in through check of degrees it is called primary check. This verification is achieved through so many different verification channels. In 2015 a fake degree selling organization named Axact was reported which was believed to sell to more than 215,000 fake degrees all over the world through a chain of approx. 350 fraud high schools and universities they made almost 51 million dollars in that year. Former FBI agent Allen Ezell, since 1980 he is investigating the fraud degrees. He told that organizations prefer paper degrees and as long as this trend is out there scams will be there in one or another [2].

Fraud degrees are often associated or they are represented with Latin words or phrase. Therefore languages on a degree certificate should be checked thoroughly. If there is some Latin word present on a degree then one should be get vigilant that degree might be fake. United Kingdom universities have stopped using Latin mentioned on degree certificates from past decade. If a university named such as Sheffield University is written instead of university of Sheffield then one should be aware of it too. One of the best way to check if a degree is fake or not is by getting actual address of mentioned university on certificate. And by using that address and search it online just to check university address legitimacy is also an effective approach to check weather a degree is fake or not [3].

Related Work

The uses of badges is getting very common in universities like Knowledge Media Institute this is an Open University of United kingdom, these badges are the certificates and a source of web reputed with use of trusted distributed ledger of blockchain. Knowledge Media Institute is exploring use of Ethereum by converting badges in to the form smart contacts which is one of the efficient way. This has developed a framework for creating micro credentials on blockchain. Knowledge Media Institute is working on project with their full attention on developing blockchain for making it in use United Kingdom education credentials and to lead blockchain projects in higher educations. Knowledge Media Institute is collaborating with United Kingdom number of other institutes like University of Ghent, University of Texas and so many others to develop blockchain network of degrees attestations. But developing his network does not considers the end users and fulfilling the needs are third party such as hiring organizations. KMI is more focused on the application layer and in simple, wallet and data keys can be controlled by users themselves. All the parties using this network can control of all the data and private keys. However understanding blockchain framework and its network complexities are not the easy tasks for average person. Such use has need of full technical support [4].

Open University is fully believes that this network of blockchain is good enough to provide degree attestation facilities to educational institution all across the United Kingdom. Privacy is top priority of this network for user. This is also end to end encrypted. But there are also issues present here because all these are linked with public blockchain. In this section there no way for blockchain to protect privacy of its end users [5]. Some universities like University of Nicosia they are using Bitcoin blockchain for many usage processes such they accept bitcoin as their online courses and many other degree programs and at the end of these course they also provide degree certificates at the end course. All the degrees certificates that are issued by University of Nicosia using bitcoin blockchain framework they are used just to remove the fake degrees frauds and also number of other payment frauds this main objective is to deal with manipulating with the numbers of students. By using bitcoin blockchain network University of Nicosia tackle the problem of fake diplomas since 2007 they also provide different kinds of software tools in order to attest the legitimacy of a degree [6].

Another blockchain based platform for digital credentials verification is SmartCert. It develops to initiate the authenticity of academic credentials on a blockchain and to master over the problem of bogus certificates. It uses the cryptographic signing of educational certificates to appreciate transparency in the case of hiring. The hash will be shared, by the student, with the prospective employer to verify the certificate. However, in the case of digitally signed certificate or hash, it can be difficult to gain access for a legitimate user because the computer that is accessing this data, can be attacked by an intruder. Another issue with this application is, data security is not ensure by cryptography, and therefore, to guard against the threats, the fundamental security measures must be implemented. Meanwhile, cryptographically secured certificates will not easily allow to fake the certificates [7].

There is another blockchain based solution to verify academic certificates, namely “RecordsKeeper”. By using this, educational institute issues certificates and receipt will be provided to user which can be shared with others (third party) to prove the authenticity of certificate in the RecordsKeeper blockchain ledger. There are less complications in this mechanism, but parties are more interested to have ownership rights instead of only view the certificate in ledger. This amount of transferring the ownership to the other may lead to tampering. Private Blockchain may work well in this case to ensure the security of certificate [8].

To tackle these fake degrees issues universities has attestations systems in their governing bodies this most this is a manual type of type of attestation system. Although this verification is somehow helping to counter fake degrees issues by this system has its limitations. These limitations are first of all it's a very time consuming system organizations have to wait for days in order to get any employee degree attested. Which is a hectic process for some organizations. Second flow is bribing the officials which are there in chain of network of attesting degrees such as universities officials. Third problem organization facing is retrieving particular records of their employee which again face the first and second problem [9].

Technical Review

What is a Blockchain?

A Distributed Ledger

Distributed ledger is core of blockchain it help to save all transfers of data between networks. It is created as decentralized form of blockchain ledger this because it creates it replicas all over its members of network, each member in network work as team together for maintaining the system. This concept of decentralization is most power full feature of this blockchain ledger and collaboration of its members across the network is cherry on top.

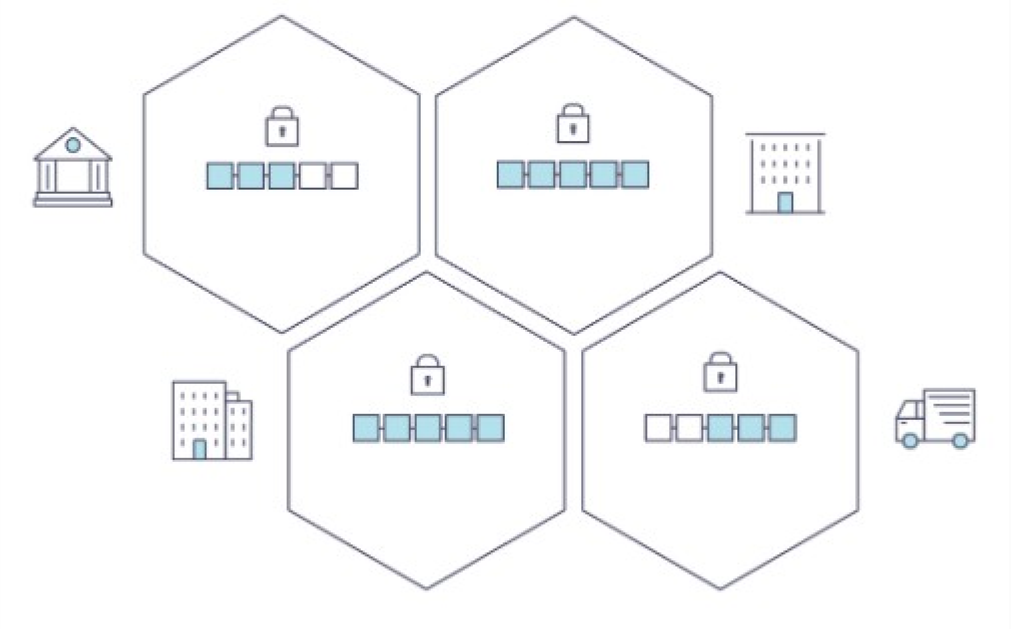

Figure 1 Blockchain Network

Cryptographic techniques gives a user full sense of surety that once a transfer is done in to the ledger it cannot be changed. This property of blockchain ledger is called immutability.

Consensus

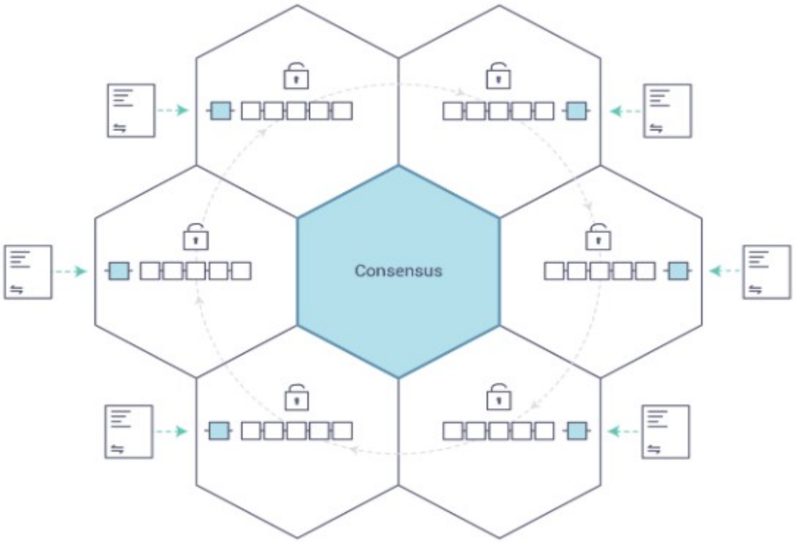

Figure 2 : Consensus

In order to keep transition of data synchronous all over the blockchain networks and to make sure the distributed ledger will only be updated when transfer are approved only some particular members, the ledger makes sure that when update is in process it must be in same order as the order of transitions this is called consensus.

Why is a Blockchain useful?

Today’s Systems of Record

Now a days the networks are more updated forms of previously existed networks as because records of business are hold in place. The participants transfer information between each other in business networks. Whether it’s an old food industry records or now updated and lasted version of today security companies’ data their transfer records of information must be kept separated.

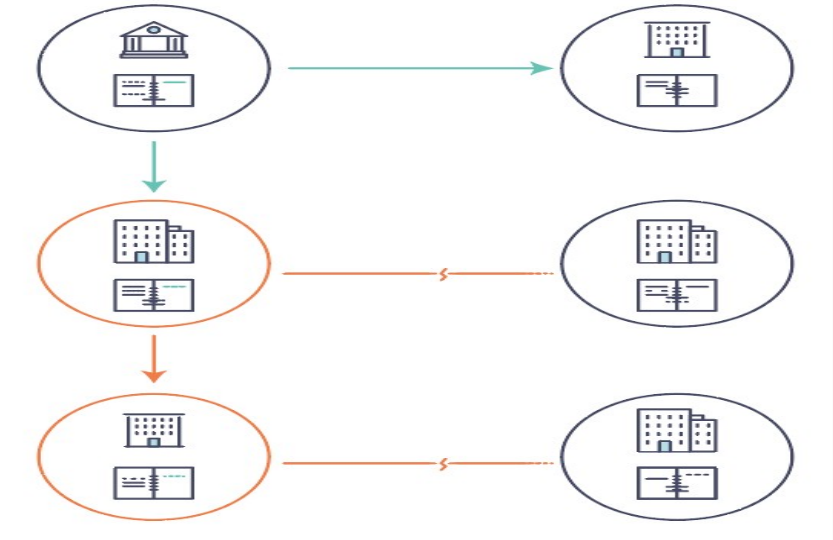

Figure 3 : System Records

We can imagine the technology advancement form this the technology has revolution from stone carving of information to hand written books in middle ages to printed manuscripts of information to the lasted for digitalization of data stored in hard drives and chip cards. Process of preserving of information is same but methods have been changed almost unimaginably. This just technology advancements in modern era.

The data banks of every modern day organization is almost different with separate protocols. With different sets of security measures from food industry to security industry. Now blockchain networking systems has made its possible of total secure transfer of information of date between interlink industries

The Blockchain Difference

Modern system of data transfer in spite of using inefficient rats nest, there are standard models for business networks to establish saving of data, identification of transfers data on networks, and transfers executions, what if worth of an assets could know by just looking at its transfer history, once transfer is done it won't be changed, therefore it can be trusted?

The blockchain network look below image, here every member has its own distributed ledger copies, In addition to this distributed ledger, information is also shared between networks. The updating processes which are used by distributed ledger are also being shared between networks. Unlike modern systems approach where private distributed ledger are updated by private distributed ledger programs. Same goes for shared distributed ledger updating as it is done shared distributed ledger program.

That present network of business would look more like this:

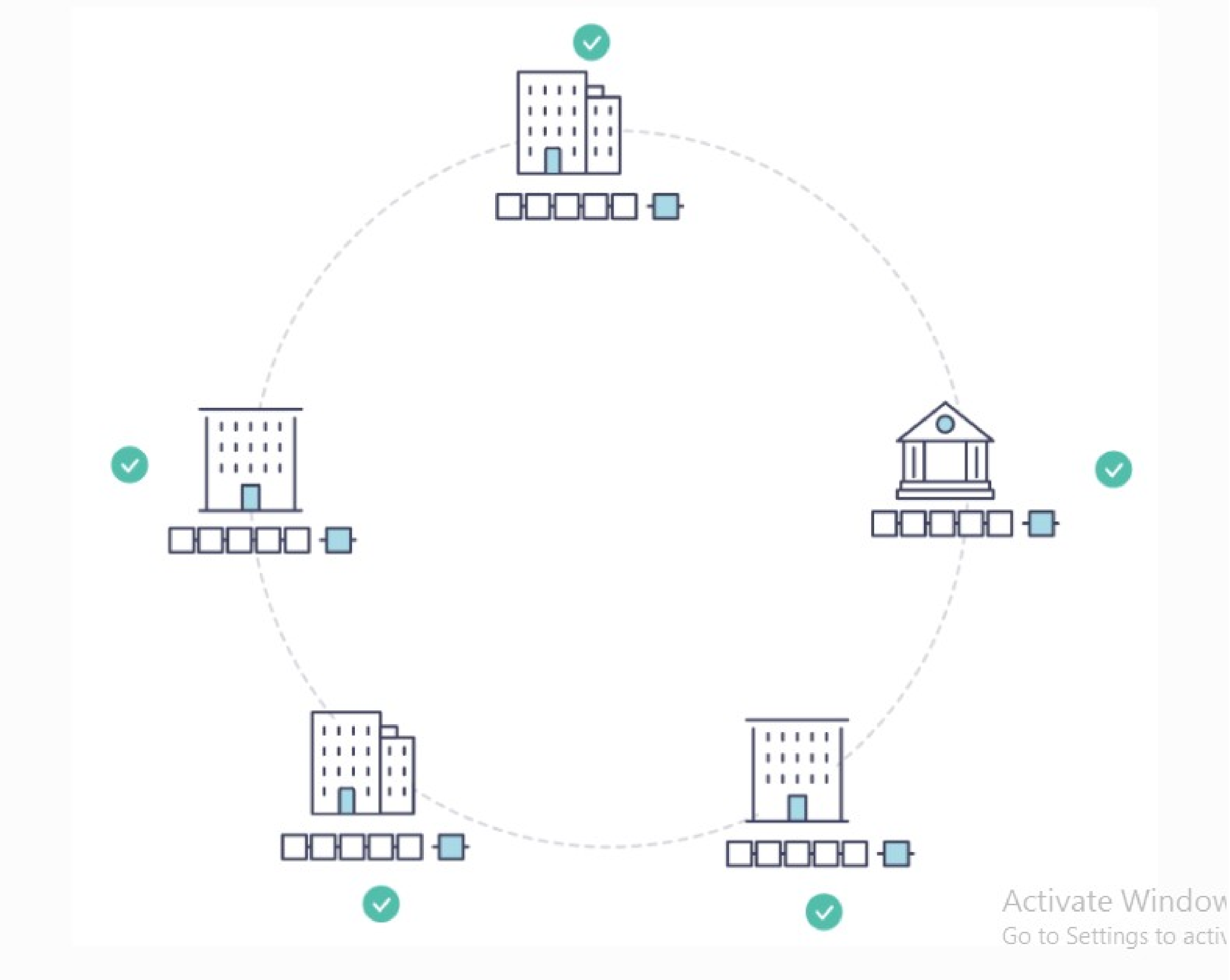

Figure 4 : Distributed Ledger

Shared distributed network of ledger helps to cut the cost, it’s also decreases the shared time transfer, it also minimizes the risk link with private data and executing number processes with improvement of reliability and visibility sideways.

There so many details that are useful which makes blockchain a very useful framework but all those details are linked with data transfer and execution of processes during sharing of network

What is Hyperledger Fabric?

In order to provide highest degree of security, strength, flexibility, endurance and scalability hyperledger provides us a framework architecture for distributed ledger. Its helps to implement different type of elements and apply their complexities across the system ecosystem.

To modernize inter linkage of organization, blockchain technologies hyperledger was developed by Linux foundation in 2015. Its specialty is that it invites communities to help in developing process in hyperledger blockchain rather following a standard unique protocol. It promotes collaborations. It also gives all the intellectual property rights to its developers.

Hyperledger Fabric is a platform within hyperledger of blockchain. It is similar to other blockchain. Hyperledger fabric puts use in smart contacts, it is a system through which member manage their transfer of data.

The dominating feature of hyperledger fabric which makes it different from other technologies is its feature of private and permission. It’s a very different than open system network which is permission less those system allow unidentified systems to take part in networks and lay their hands on data and transfer. The participants in hyperledger fabric network they enter in network through a special pass called membership service provider (MSP)

Its data can be stored in multiple formats. It’s also has so many pluggable options. The mechanisms of consensus can be used in and out, there are also numbers of different membership service provider (MSP) which are supported.

Hyperledger fabric has a feature of creating different channels, which gives ability to its member in network to make their own separate transactions.

Hyperledger Fabric also offers the ability to create **channels**, allowing a group of participants to create a separate ledger of transactions.

Shared Ledger

This hyperledger fabric system consist of two parts. First part is called world state and the second part is called transaction log. Every member in hyperledger fabric systems network has its own copy of the system it belongs.

Hyperledger fabric systems networks database is world state, it is also the description of state of the system in which it is currently in. The present value of system is recorded in transaction log.

This is updating history for the hyperledger fabric world state. The combination of both these part world state and transaction log makes the complete ledger network.

All the information saved in world state is replaceable. The transfer of data log is always pluggable. The past and future value are recorded in ledger databases which are places in hyperledger fabric blockchain network system.

Smart Contracts

Chaincode in hyperledger fabric system consist of smart contacts they are executed in blockchain by external application that interacts with hyperledger fabric. Chaincode almost in every case is related and work with parts of database in the ledger. Not in transfer log but just in world state. Many programming language are used in implementation of chaincode. Golang are also supported by it.

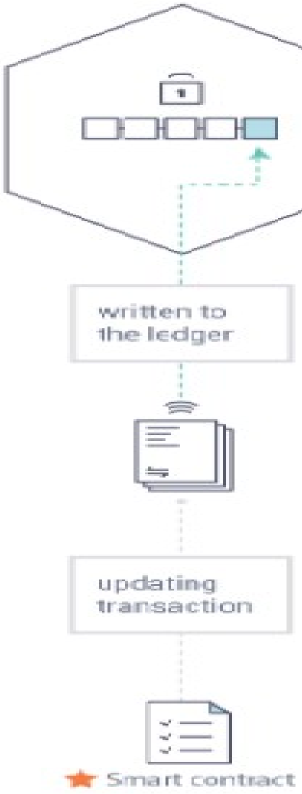

Figure 5 : Smart Contracts

Client SDK

The Client SDK in hyperledger fabric is use to interact with a Hyperledger Fabric blockchain with the help of APIs. It provides a simple API to invoke chaincode methods for submitting transactions to a ledger or query the contents of a ledger. Client-SDK-Nodejs uses the npm & NodeJS to invoke chaincode methods.

NodeJS

Node.js is an open source JavaScript framework its features include that its API's are Asynchronous and Event Driven. Its waits for an API to return back to server. Server then shifts to next API after calling it. Its features also include that is a very fast frame work it has very high code execution rate. Its other feature include that it is a Single Threaded framework but also Highly Scalable framework too. Its use single threaded frame by looping events. One of its performance features include no buffering of data**.**

Express JS

Express is an open source back end web application and it the framework for Node.js. It helps to explore of use and a full feature set. Express deals with all the interactions between the frontend and the database, ensuring a smooth access and transfer of data to the end user. It is designed for to be used with Node.java script and so carries on the in-tune use of JavaScript all over the stack.

Express is complete package it is designed to effectively control processes without messing up application. APIs for the frontend will be creating using express routes.

Angular JS

Angular is a structured framework for web applications. It is Google's JavaScript frontend framework and not the only frontend framework in use, but it is very popular. It extends HTML attributes along with **Directives. Also, it** binds data to HTML with **Expressions**. Its main goals are simplification and structuring of JavaScript code. Angular is a powerful frontend framework so there are many reasons to use this framework such as Major community, Readable code, Google as creation, Customizable, Flexible, Pre-made solutions, easy testing, etc.

RESTful API and its working

A RESTful API is a web infrastructural style for an application program interface (API) in to order to access and use data its use the requests from HTTP. This data will be used to GET,PUT, POST and DELETE key data types, GET key data type refers to reading of data , PUT key data type refers to updating data, POST key data type refers to creating data and last DELETE key data type refers to deleting of operations concerning resources. Five types of data formats is supported by the REST API that are application/xml, application/x-www-form-urlencoded, application/x-wbe+xml, application/json, and application/json. The most commonly used formats are application/xml & application/json

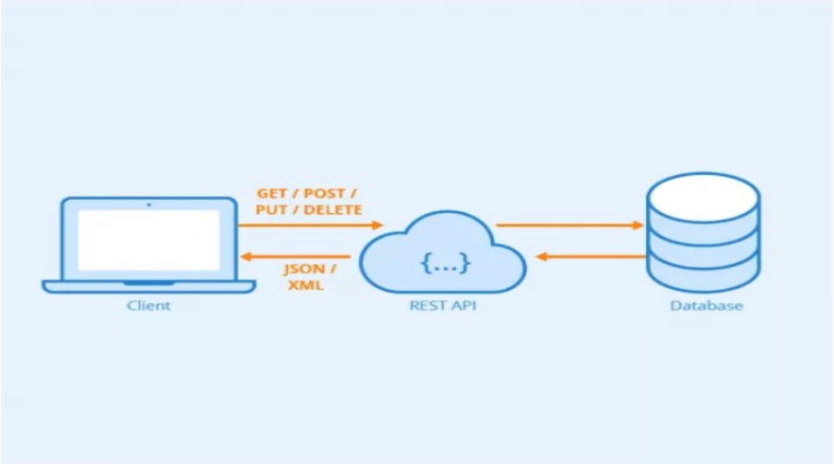

Figure 6 : REST API

Uses of REST API

The main advantage of using it stateless calls that helps to reconstruct a code if anything falls apart that is why RESTful API is very useful in cloud applications. The redeployed structure can be scaled up and down according to needs to comply with new made changes, it’s just because requests are unpredictable, and they can be directed in any direction or component instances. There is no present saved data which can remembered for next transaction. That is why Rest is widely used for web.

RESTful API Design and Architecture Constraints

In order to be a true RESTful application program interface, a web developing service must meet to the following six REST structural constraints:

1. **Uniform Interface:** the constraint name applies, it must be decided that APIs interface for resources inside the system which will be exposed to API consumers. All the resources should use a common approach to access such as HTTP GET and similarly modify with the use of a consistent approach.
2. **Client-server:** This constraint basically means that the server application & the client application should be able to evolve separately without having any dependency on each other. Only URIs should be known by client, and that's all.
3. **Stateless:** All client-server interactions should be stateless. The server should not store anything about the client made latest HTTP request. Every request should be treated as new. No history, no session.
4. **Cacheable:** In REST, caching shall only be applied to resources when it is applicable, and then the resources should declare themselves cacheable. Server or client-side, both can implement the caching.
5. **Layered on demand**: A layered system architecture is used by the REST that allows one to deploy the APIs on server X and store the data on server Y and request authentication done in Server Z. For example, a client will not be known that whether it is connected directly to the end server or it is connected to the intermediary along the way.
6. **Code on demand (optional):** Most of times, the static representations of resources is sent in the form of XML or JSON. But one is free to return executable code (i.e. UI widget rendering code) to support a part of application, then it is permitted.

Requirements

System Requirements

We will explore the various aspects of the system related to developing the system in the complete product. These are the conditions that must be met for the success of the project. It provides a straightforward way to perform the tasks. If you collect project requirements effectively, you can reduce the total cost of the project, you can increase the project success rate and effective communication between key participants. The main purpose of the project is to develop and implement a certification verification system.

External Interface Requirements

This section will explain the detailed information of the developed system and all its components, as well as its functional requirements for the system.

Software Interface

User can apply for degree on University's system using DVS. After getting the request of degree from users, university verified the students record and issue the degree after verification.

Functional Requirements

Functional Hierarchy

blockchain based system

- Admin can create users of type admin, examiner, endorsers (Vice-chancellor & pro-chancellor)
- Admin can activate/de-active user.
- Examiner can add new student data.
- Examiner can edit student data.
- Examiner can delete student data.
- Examiner can view student data.
- Endorser can view student data.
- Endorser can endorse student data.
- Endorser can reject student data.
- Endorser can view all pending request.
- Endorser can view all rejected students list.

- Endorser can view all his endorsements.
- Verifier can view student data by ID.
- Verifier can view student digital degree.

Requirement Prioritization

As client anticipations are lofty and limits are strict, you ought to make up really the development team presents the extremely useful characteristics as swiftly as possible. Prioritizing is the only means to join the conflicting needs of constrained assets.

MoSCoW Method

Moscow analysis is very important to prioritize the project management. To understand the dynamic system, we can look at its biggening by understand the Moscow method: It is designed by professional to make it better in quality products and rapid development of application process. In the first phase, understand the features of dynamic system development method to follow them strictly to maintain the quality, cost and time in project development. Entire development responsibilities must be allocated built on their status. The necessary disciplined significances has preceded to the advancement of a separate order form.

The shortened structure of MoSCoW is inscribed with the initial missive of the implying unit applied with it. These must have, should have, may have and should not have. In that manner, you can describe which job is of that sort.

Prioritization Rules

These strategies or situations assess the significance of any duties, processes, techniques, etc. Each firm or work group embraces its specific technique of establishing terms, although they are not extremely unique. The features are as follows.

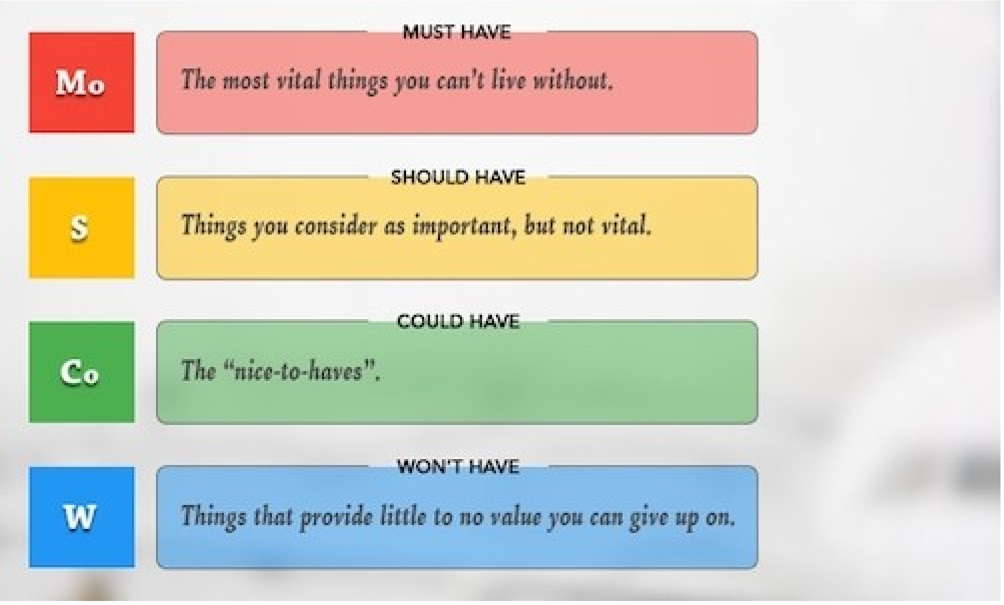
MUST HAVE
Mo
The most vital things you can't live without.
SHOULD HAVE
S
Things you consider as important, but not vital.
COULD HAVE
Co
The "nice-to-haves".
WON'T HAVE
W
Things that provide little to no value you can give up on.

Figure 7 : MoSCoW Method

Must Have

It has blockchain based system. Admin can create users of type admin, examiner, endorsers (Vice-chancellor & pro-chancellor). Examiner can add new student data. Examiner can edit student data. Examiner can delete student data. Examiner can view student data. Endorser can view student data. Endorser can endorse student data. Endorser can reject student data. Endorser can view all pending request. Endorser can view all rejected students list. Endorser can view all his endorsements. Verifier can view student data by id. Verifier can view student digital degree.

Should Have

Users should be able to change their password. Admin should be able to active/de-active user. When examiner change the student data, all endorsements should be removed. Endorser should add reason while rejecting the data.

Could Have

Blockchain system can run on a single machine by creating multiple instances. Functionalities could be performed by mobile app browser.

Would Not Have

Deployment on cloud using multiple nodes.

Non-Functional Requirements

In this topic, we analyze how the system will perform a certain function or task. How will the system behave in certain circumstances and what are the limitations of its functions?

Safety Requirements

It can happen that major damage to the main body of the database as a result of a disaster can crash on the hard drive. In this case, the recovery method can restore a previous copy of the database that was backed up in the storage archive and rebuild it to a more current state by re-applying the transactions involved in the backup or until the moment of failure. to do.

Security Requirements

The security system, like any other application, requires storage in the database. However, the special demands of the security market mean that service providers have to carefully select their partners in the database.

Software Quality Attributes

Usability: The system should be accessed by the maximum number of users without any problems.

Availability: Our project will be presented on the server, so it must be always available to the user.

Maintainability: The system should always maintain its correct position, it should change to correct faults and errors, it should improve its functionality and performance, and it should adopt in a modified environment.

Correctness: The system must provide accurate reports as intended and act correctly during any particular task.

Use-case Diagrams

It shows the user interaction with system, it is a graphical depiction. It has many users and use cases. In these use case diagrams, there are users that interact with system.

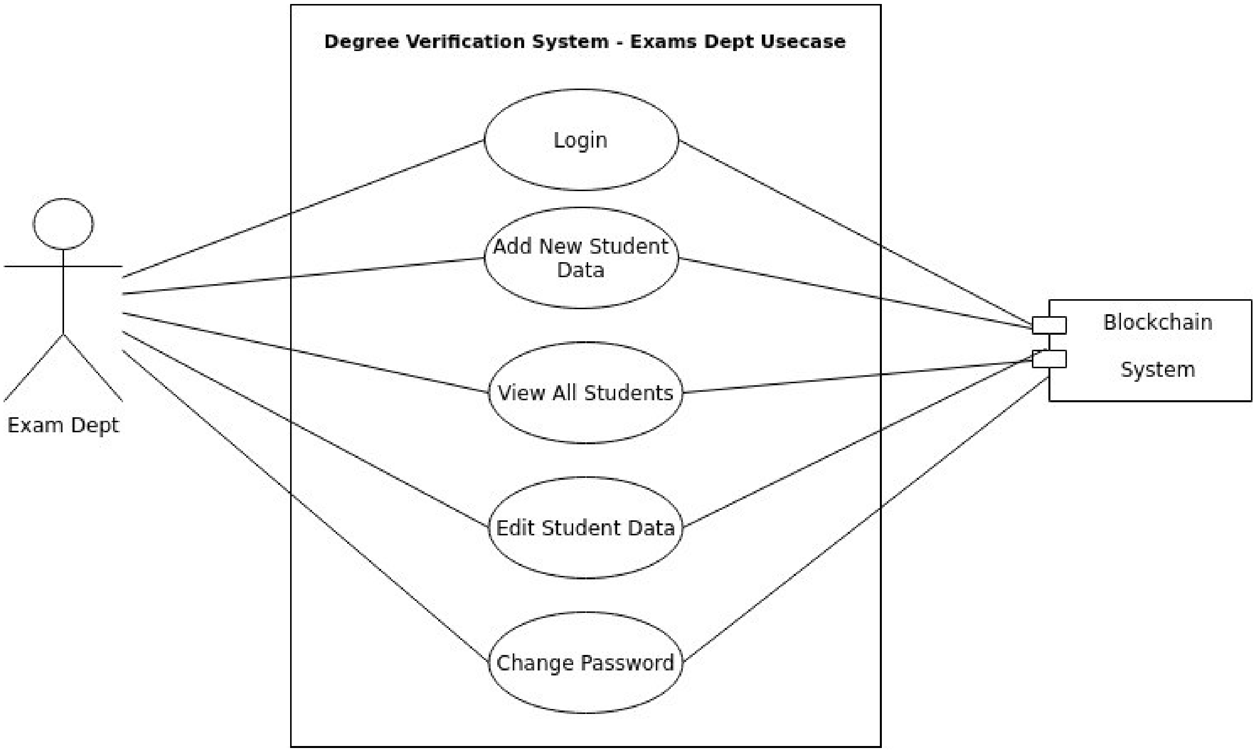

Figure 8 : Use Case Diagram [1]

ID:	**Exam Dept Use Case**
Title:	Exam Dept
Description:	This use case allows users to login to the system.To login to the system, users need to have a DVS account. Using the credentials of DVS account, users will be able to use the system.
Primary Actor:	Exam Dept
Preconditions:	User must have a DVS account
Postconditions:	1. The system displays a dashboard
Main Flow Success Scenario:	1. The user clicks the login button 2. The screen redirects to Blockchain link 3. The user enters his credentials (i.e. email & password) 4. The system displays the dashboard 5. The use case ends
Alternative Flow	3a Missing email ID or password 1. The system prompts for email ID or password. 2. Use case resumes at main flow step 1 3b Invalid DVS account credentials 1. The system displays the invalid credentials error message. 2. The system prompts for email ID or password. 3c Not any DVS account 1. The system displays the error message to the user regarding to that there is no such account. 2. The systems redirect to the login page.

Table 1: Use Case Description [1]

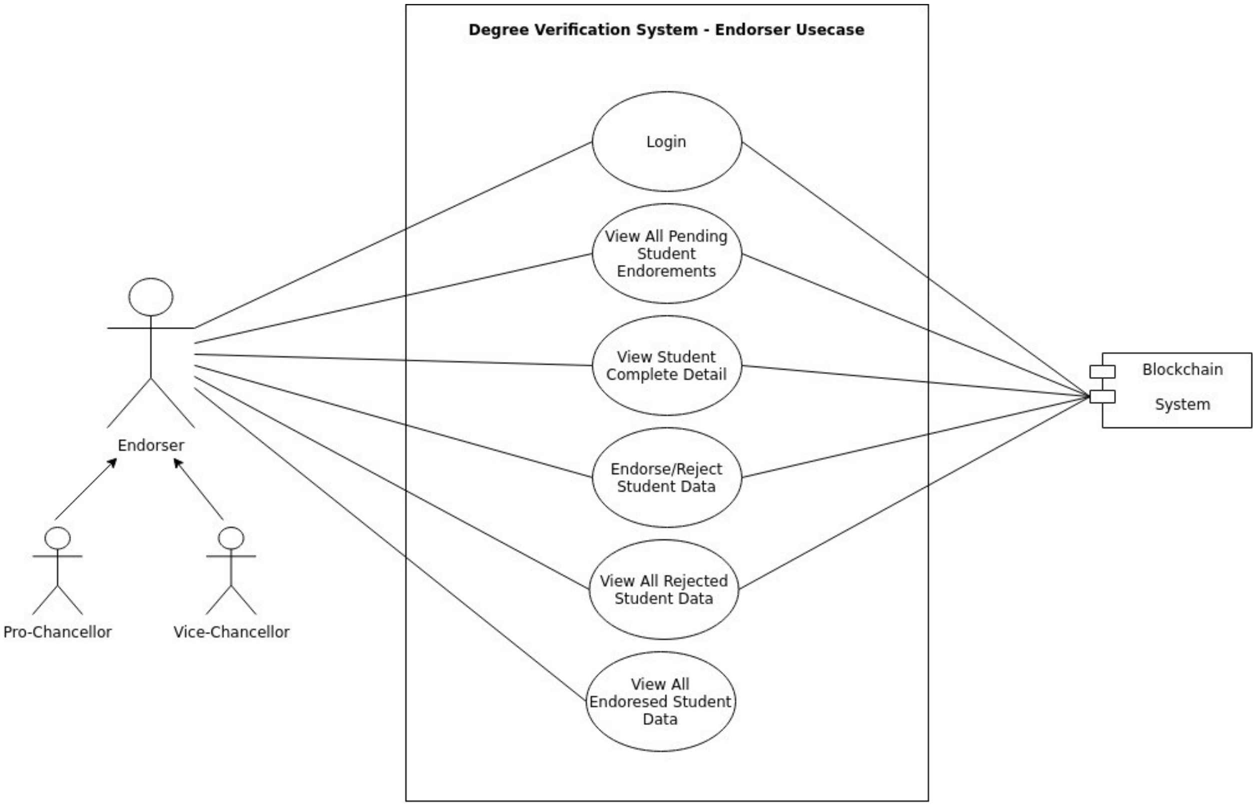
Degree Verification System - Endorser Usecase
Login
View All Pending Student Endorements
View Student Complete Detail
Endorse/Reject Student Data
View All Rejected Student Data
View All Endoresed Student Data
Endorser
Pro-Chancellor
Vice-Chancellor
Blockchain System

Figure 9 : Use Case Diagram [2]

ID:	**Endorser Use Case**
Title:	Endorser
Description:	This use case allows endorser to login to the system.To login to the system, users need to have a DVS account. Using the credentials of DVS account, users will be able to use the system.
Primary Actor:	Endorser
Preconditions:	Endorser must have a DVS account
Postconditions:	2. The system displays a dashboard
Main Flow Success Scenario:	6. The endorser clicks the login button 7. The screen redirects to a link 8. The endorser enters his credentials (i.e. email & password) 9. The system displays the dashboard 10.The use case ends
Alternative Flow	3a Missing email ID or password 3. The system prompts for email ID or password 4. Use case resumes at main flow step 1 3b Invalid DVS account credentials 3. The system displays the invalid credentials error message 4. The system prompts for email ID or password 3c Not any DVS account 3. The system displays the error message to the user regarding to that there is no such account 4. The systems redirect to the login page.

Table 2 : Use Case Description [2]

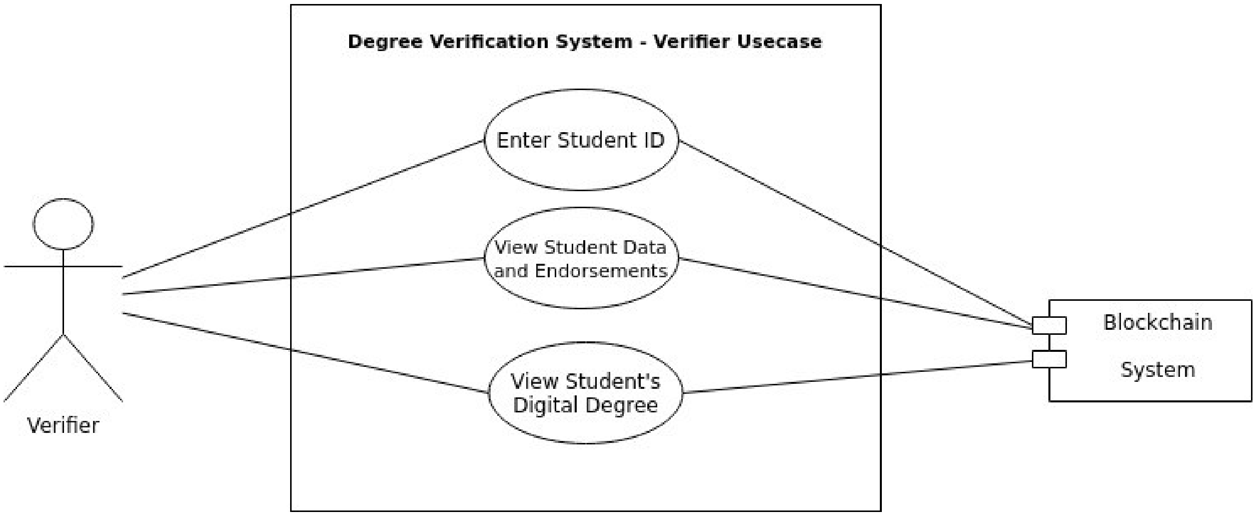
Degree Verification System - Verifier Usecase
Enter Student ID
View Student Data and Endorsements
View Student's Digital Degree
Verifier
Blockchain System

Figure 10 : Use Case Diagram [3]

ID:	**Verifier Use Case**
Title:	Verifier
Description:	This use case allows verifier to enter student ID to the system. By entering the Student ID verifier can verify the student degree or endorsement. Verifier can see the student digital degree.
Primary Actor:	Verifier
Preconditions:	User must have access to DVS.
Postconditions:	3. The system displays a dashboard
Main Flow Success Scenario:	11. The user enters the student ID to verify. 12. The screen redirects to view student data or endorsement. 13. The user can see the digital degree of student.
Alternative Flow	3a Missing Student ID 5. The system prompts for invalid student ID. 6. Use case resumes at main flow step

Table 3 : Use Case Description [3]

Design

A software design must describe the architecture of the system, i.e., how the system is broken down and organized into components and must describe the interfaces between these components. You must also describe these components in an appropriate level of detail to allow their construction.

The process of defining the architecture, components, interfaces and other features of a system or component and the outcome of the process. Viewed as a process, software design is the activity in the software development lifecycle in which software requirements are analyzed to produce a description of the internal structure and organization of the system that will serve as the basis for its construction.

Software design is an important component of the product growth phase.

In the design stage, the visualization of the real solution is created, i.e. a detailed program architecture is created that meets the specific requirements of the project.

Custom software design by architects and software engineers defines specific workflows and standards and includes an end-to-end solution / clear product design, along with database structure and design. At this stage, the entire structure of the project was built using the final prototype and models used for the next phases of the software development process.

This chapter comprises of class diagram, activity diagrams, and sequence diagrams.

Class Diagram

Class diagram is a blueprint of any project. It shows the behavior of objects with each-others. Each object has data that is modelled, and it is crucial part of object oriented modeling. It shows system classes, their attributes, operations and, relationships among them. It also shows that how data is delivered through and display general concept model of developed application.

In below figure there are five classes, each class has its attributes, data, properties and operations.

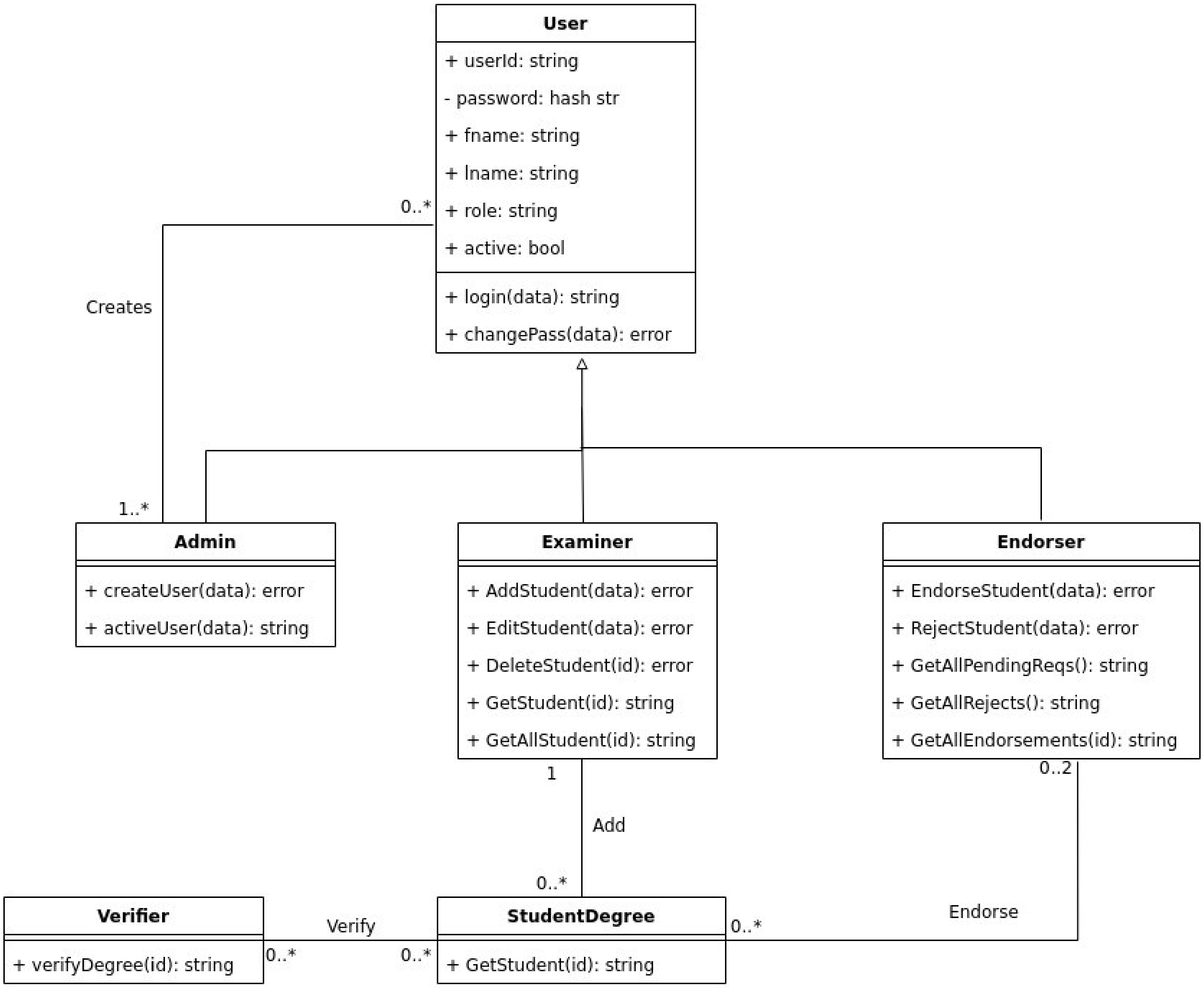
User
+ userId: string
- password: hash str
+ fname: string
+ lname: string
+ role: string
+ active: bool
+ login(data): string
+ changePass(data): error
0..*
Creates
1..*
Admin
+ createUser(data): error
+ activeUser(data): string
Examiner
+ AddStudent(data): error
+ EditStudent(data): error
+ DeleteStudent(id): error
+ GetStudent(id): string
+ GetAllStudent(id): string
Endorser
+ EndorseStudent(data): error
+ RejectStudent(data): error
+ GetAllPendingReqs(): string
+ GetAllRejects(): string
+ GetAllEndorsements(id): string
1
Add
0..*
0..2
Endorse
0..*
Verifier
+ verifyDegree(id): string
Verify
0..*
0..*
StudentDegree
+ GetStudent(id): string

Figure 11 : Class Diagram

Sequence Diagram

Sequence diagrams show the interaction of objects in order in which these occurs. Sequential diagrams are interactive diagrams that detail how operations are performed. They capture the interaction between objects during collaboration. Sequential diagrams are a time focus and visually display the order of interaction using the vertical axis of the diagram to represent when and when messages are sent. The interaction that takes place in a collaboration that either creates a use case or a process. Extreme-level collaborations amongst the structure user and the procedure, amongst the system and other structures.

In blow figure, it shows that an object verifier interacts with system to verify the student data.

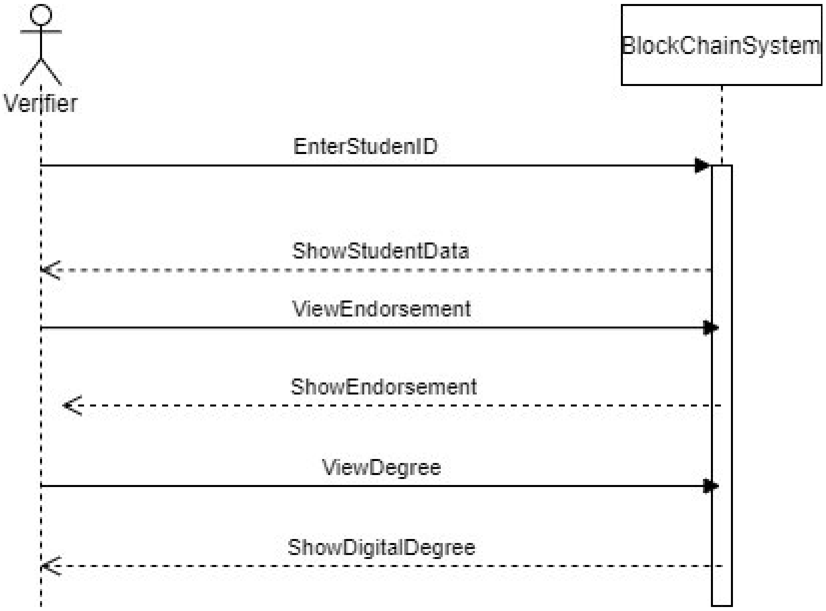

Figure 12 : Sequence Diagram [Verifier]]

In figure below, it shows the interaction between an object named ExamDept with system object and exchange data among them.

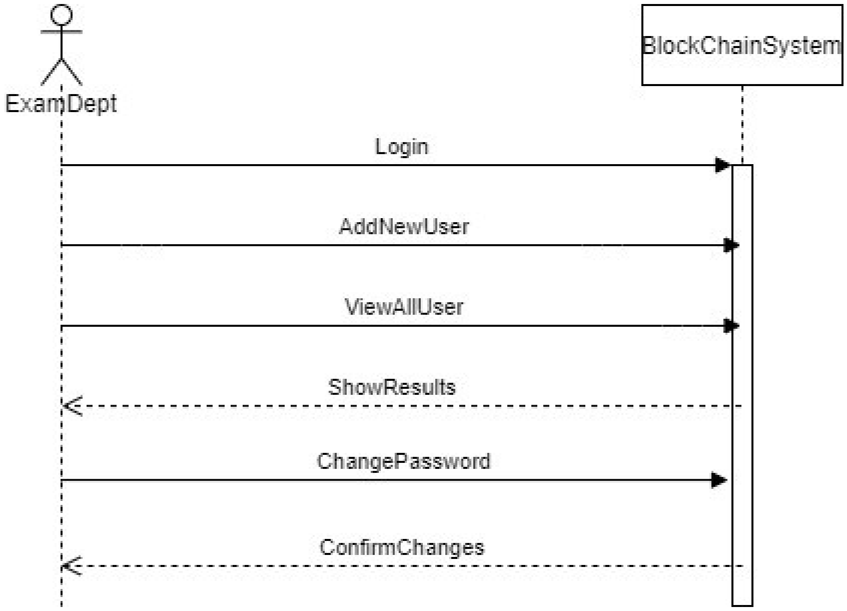

Figure 13 : Sequence Diagram [ExamDept]

In figure below, it shows the interaction between an object named Endorser with system object and exchange data between them.

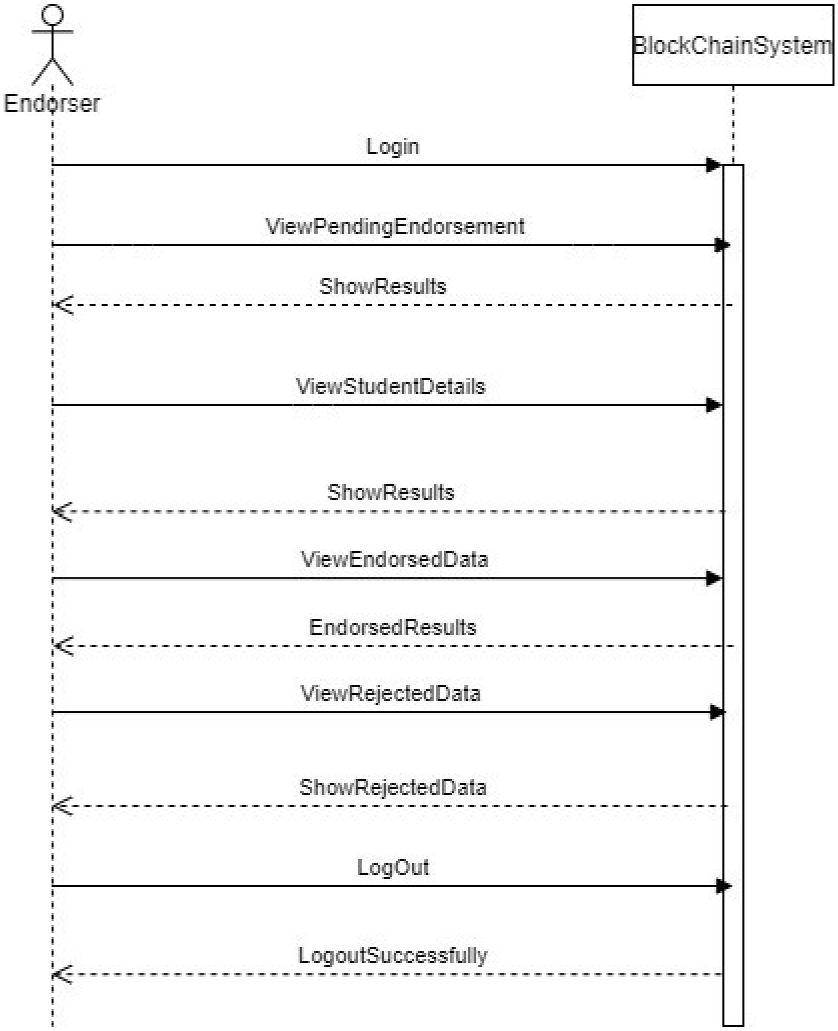

Figure 14 : Sequence Diagram[Endorser]

Activity Diagram

The activity diagram is another important behavior diagram in the Unified Modeling Language diagram to describe the vibrant characteristics of a system. An activity diagram is essentially an enhanced edition of a diagram that plans the movement from one action to an alternative.

Activity diagrams describe how activities are coordinated to provide a service that can be at different levels of abstraction. Typically, an event must be done over a certain procedure, particularly when the resolution of the procedure is to achieve a quantity of diverse possessions that need management or how the events in the case of a use are related to each other, especially in cases where activities may overlap and require coordination.

This figure shows that an activity is performed to login the system. Steps involves are enter username, enter password, and check role.

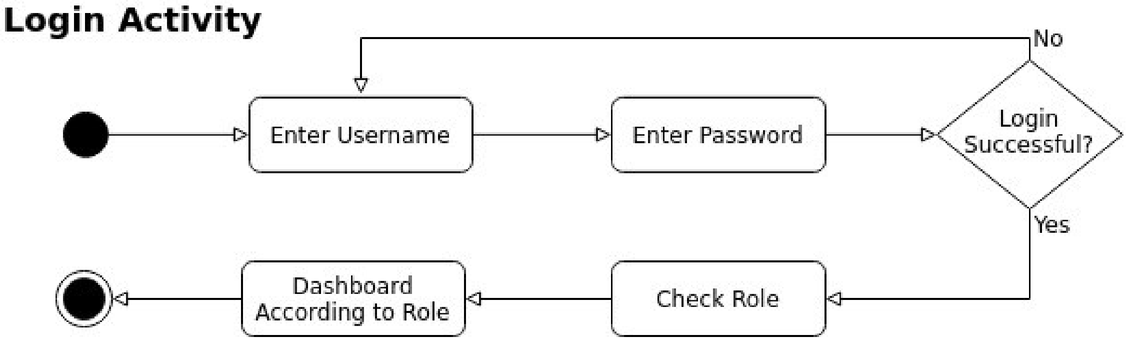

Figure 15 : Login Activity

In this figure admin create the new user, its details and other credentials. Steps involves are admin login, enter user details, select role, set password.

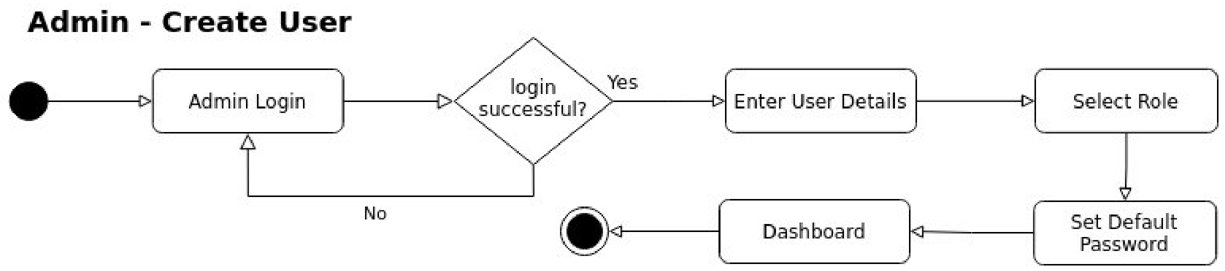

Figure 16 : Admin Create User

In this figure, examiner add the new student data for endorsement. Steps involves are login, add student data, submit request, show students.

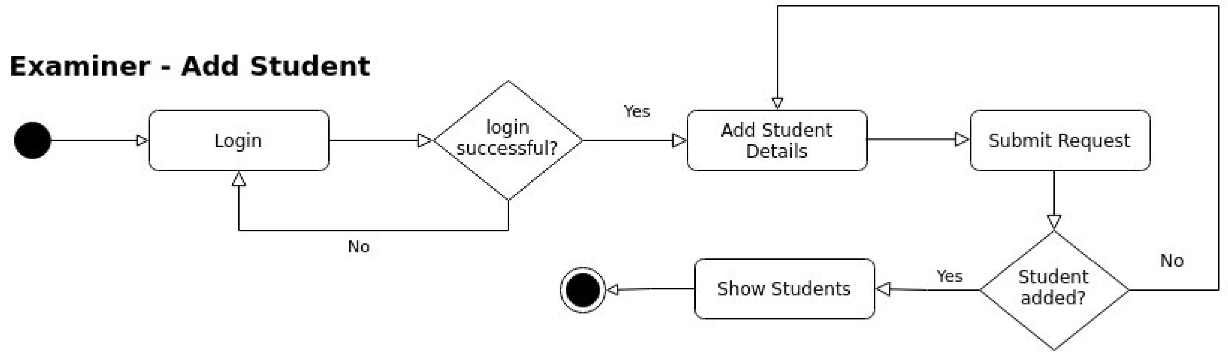

Figure 17 : Examiner Create Student

In this figure examiner can edit the student record. Steps involves are login, get student details, edit student data, submit request, show students.

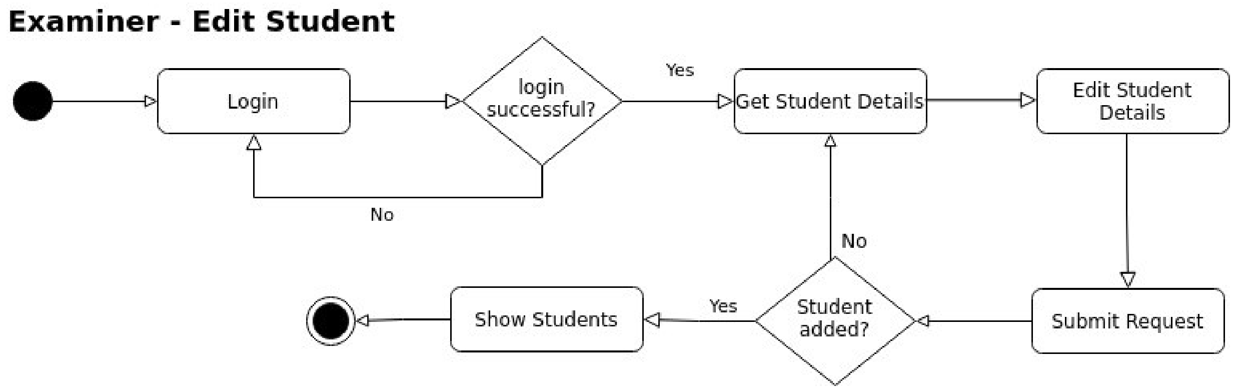

Figure 18 : Examiner Edit Student

In this figure endorser can endorse the student data. Steps involves are login, show students, select student data, endorse data, show endorsement.

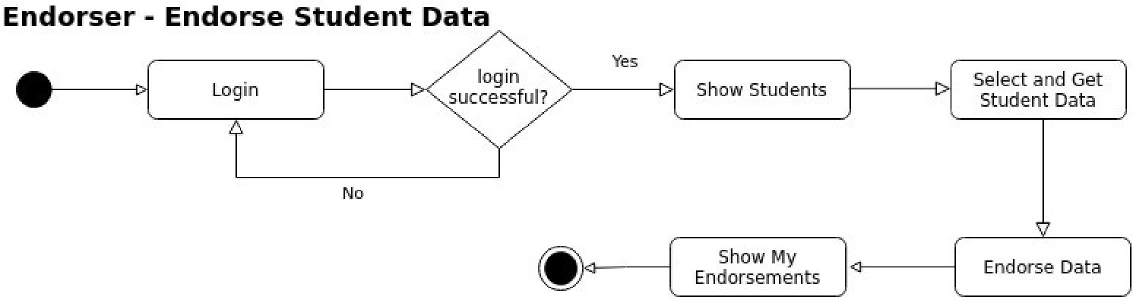

Figure 19 : Endorse Data

This figure shows that endorser can also reject the data it is not correct. Steps involves login, show students data, reject endorsement, reject reason, show endorsements.

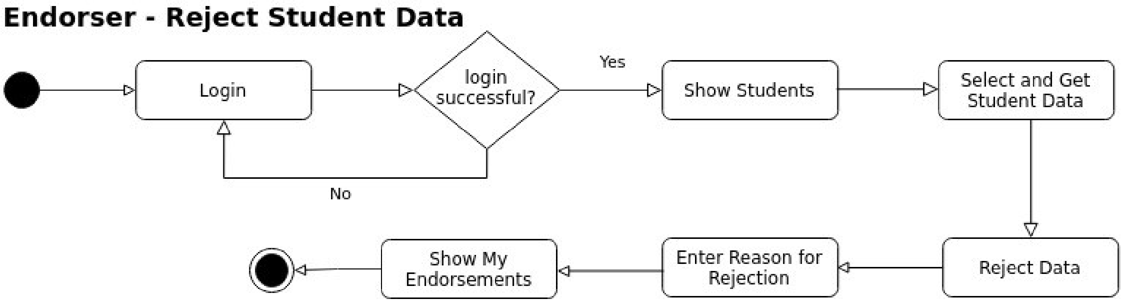
Endorser - Reject Student Data
Login
login successful?
Yes
No
Show Students
Select and Get Student Data
Reject Data
Enter Reason for Rejection
Show My Endorsements

Figure 20 : Reject Data

This figure shows that verifier can verify the student data for endorsement. Steps involves are enter student ID, show student data, show endorsement, show degree.

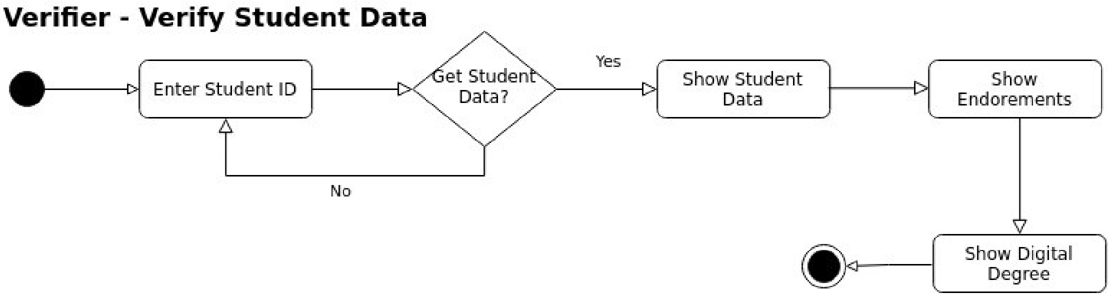

Figure 21 : Verify Data

Implementation Plan

Methodology

An agile model will be followed to achieve the objectives. The agile model believes that each project should be treated differently and that existing methods should be adapted to better meet the requirements of the project. In Agile, tasks are broken down into deadlines (small deadlines) to provide specific functionality for a release. An iterative approach is adopted and the construction of the functional software is provided after each iteration. Each build is incremental in terms of functionality; the final construction contains all the characteristics required by the end-user.

Agile vs. Waterfall vs. Kanban vs. Scrum

- The Waterfall works best for projects that are completed linearly and do not allow it to return to an earlier phase.
- Agile concentrates on synchronized and adaptive systems. Agile methods split plans into shorter, reiterative phases.
- Kanban is particularly apprehensive about procedure enhancements.
- Scrum makes work faster.
- Water is a chronological lifecycle model, while Agile is a unceasing repetition of expansion and assessment throughout the software growth procedure.
- Compare the methodology waterfall and agile, which follow an incremental approach, while the Waterfall is a sequential design process.
- Agile allows changes to the project development requirement, while Waterfall does not have the chance to change the requirements once the project development begins.

Work distribution

Gantt chart

	Week 1	Week 2	Week 3	Week 4-9	Week 10	Week 11-18	Week 19-22	Week 23-26	Week 27	Week 28
Task 1	Project Idea									
Task 2		Supervisor allocation								
Task 3			Fix Proposal							
Task 4				Requirements						
Task 5					Initial Report					
Task 6						Main Development				
Task 7							Final Development			
Task 8								Final Write-up		
Task 9									Final Report	
Task 10										Viva

Table 4 : Work Distribution

Future Work

As we have already discussed that we are going to make it a web application which can be accessed through internet without any hardware constraint. This can target more and more audience and people can benefit from it.

Future we will develop a mobile application and involve more department to facilitate the student at their doorsteps.

We will increase the scope of project by developing other important features of project by examine the feasibility of deliverables to make it fully functional product.

Conclusion

This report has discussed the development of a Degree Verification system through a new blockchain technology. The objectives of this system to develop a new and more secure system through which more important data can be verifies and validated through a proper channel that is authentic. So, we Develop DVS to provide all the features in a single fully functional and developed system. We have discussed all the main features and their characteristics to make it more specific an personalize the system.

Degree and transcript play an important role in the life of students in many ways like finding a job or getting admission for higher education. These academic credentials like degree, certificates or transcript issued by the academic institutions. Authorities manage their records manually or semi-manually and there is no any secure way to verify whether the document is real or fake. Also, in all over the world, there are many cases has been registered regarding to fake degrees.

Verification of degree is also a challenging task; one has to send degree to the respective university to get the verification of any candidate. It also takes lots of time. However, the new technology namely blockchain, is introduced which provides a secure way to store transactions in distributed ledger. It can resolve the degree issuing and transcript mechanism.

The key benefit of using this technology is to verification will be easy and faster.

References

[1] https://www.nd-center.com/2008/01/problems-of-fake-degrees.html

[2] https://www.bbc.com/news/uk-42579634

[3] https://www.qualificationcheck.com/4-ways-to-identify-a-fake-degree-certificate/

[4] J. Domingue, “Blockchains as a Component of the Next Generation Internet,” 2017.

[5] OMAR S. SALEH, OSMAN GHAZALI, MUHAMMAD EHSAN RANA “BLOCKCHAIN BASED FRAMEWORK FOR EDUCATIONAL CERTIFICATES VERIFICATION”

[6] “The Global Universities embracing cryptocurrency.pdf.”

[7] R.G. and M.K.S. Sharma, P. Pathak, “Blockchain imperative for educational certificates,” 2017.

[8] “Upload and verify academic certifications over RecordsKeeper,” 2018.

[9] C.F. Bond, F. Amati, and G. Blousson, “Blockchain, academic verification use case,” 2015.