IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

BLOCKCHAIN BASED ACADEMIC CERTIFICATE AUTHENTICATION SYSTEM

[1]PRIYANKA KILLEDAR, [2]PRANAV L M, [3]NACHIKETH S BHAT, [4]RAVI MATH, [5]SHRUTHI SHETTY J

[1]Student, [2]Student, [3]Student, [4]Student, [5]Assistant Professor

[1,2,3,4,5] Department of Computer Science and Engineering

[1,2,3,4,5] Alva's Institute of Engineering and Technology, Mijar, India

Abstract: In this era of digitalization, most of the organizations among all sectors use web-enabled systems to produce services to their purchasers with efficiency and even folks are comfy sharing their info online, which lead to the emergence of Digital Records. for college kids, educational certificates unit the foremost important documents issued by their universities. However, as a result of the availability methodology is not that clear and verifiable, pretend certificates are merely created. A skillfully generated pretend certificate is often arduous to notice and may be treated because of the original. sure, series of solutions are planned to resolve the determined problems, that embrace utilizing a multi-signature theme to authentication of certificates. This paper explains the way to enhance the certificate verification method mistreatment blockchain technology. the form of the certification style is fairly simple. Admin can have solely access to convert physical certificate to digital certificate and stores it's inside blockchain dealing. A dealings output may be a certificate Id and it's assigned to the recipient. These Ids are often sent to anyone meant to examine or demonstrate the digital certificate.

Index Terms **– Certificate, Blockchain, Cryptocurrency, Ethereum**

I. INTRODUCTION

According to, educational certificates are extremely reputable as they function as associate indicators of the human capital of their bearers. Human capital refers to the abilities, competencies, information, and aptitudes achieved through education. educational qualifications are significantly vital working things as they function as a guarantee of not simply the information, experience, and skills of the holders however additionally of their talents, responsibility, and dedication. From the attitude of the bearers, found a correlation between academic attainment levels and higher employment prospects, and economic security. recognized that educational qualifications are deemed to be real after they are presented by a university genuine when they are approved to award such certificates.

Because they are thus valuable, people often lie about their academic qualifications by producing fake certificates. mentioned that within us there are presently a pair of million faux degree certificates in circulation and three hundred unauthorized universities operational. indicated that the United States has a very large number of fake institution establishments within the world followed by the UK that has concerning 270 fake institutes. Healy (2015) found that up to thirty-fifth of candidates in Australia falsified their educational credentials for the sake of employment. discovered that almost all candidates lie a minimum of concerning some a part of their academic credentials and skill. mentioned that educational certificate fraud prices employers concerning $ 600 billion per annum.

To overcome this, we tend to mistreatment we are using technology known as Blockchain. Blockchain is that the backbone Technology of the Digital Crypto Currency Bitcoin. The blockchain could be a distributed info of records of all transactions or digital events that are dead and shared among taking part parties. every group action is verified by the bulk of participants of the system. It contains every single record of every group action. Bitcoin is that the hottest cryptocurrency associate example of the blockchain. Blockchain Technology initial came to light-weight once someone or a cluster of people name 'Satoshi Nakamoto' revealed a report on "Bitcoin: A peer to look electronic money system" in 2008. Blockchain Technology Records group action in Digital Ledger that is distributed over the Network so creating it incorrupt. something important like Land Assets, Cars, etc. is recorded on Blockchain as a group activity.

1.1 Building trust with Blockchain:

Blockchain enhances trust across a business network. It's not that you just can't trust those with who you conduct business with it's that you just don't got to once in operation on a Blockchain network. Blockchain builds trust through the subsequent 4 attributes.

• **Distributed**: The distributed ledger is shared and updated with each incoming group action among the nodes connected to the Blockchain. All this can be worn out real time as there's no central server dominant the information.
• Secure: there's no unauthorized access to Blockchain created attainable through Permissions and Cryptography.
• **Transparent**: as a result of each node or participant in Blockchain contains a copy of the Blockchain information, they need access to all or any group action information. They themselves will verify the identities while not the requirement for mediators.
• **Consensus-based**: All relevant network participants should agree that a group action is valid. this can be achieved through the utilization of agreement algorithms.
• **Flexible**: good Contracts that are dead supported bound conditions may be written into the platform. Blockchain networks will evolve in pace with business processes.

1.2 Benefits of Blockchain Technology:

• **Time-saving**: No central Authority verification is required for settlements creating the method quicker and cheaper.
• **Cost-saving**: A Blockchain network reduces expenses in many ways in which. No would like for third-party verification. Participants will share assets directly. Intermediaries are reduced. group action efforts are reduced as each participant contains a copy of the shared ledger.
• **Tighter security**: nobody will temper with Blockchain information because it is shared among a lot of Participants.

1.3 Problem Statement

Finding the right candidate for the job when hiring has been a difficult work for employers or HRs of a company. One of the significant issues is the fake credentials given by the candidate like certificates. According to the survey of HireRight, about 56% of the educational credentials provided for background verification had discrepancies. Due to this, an eligible candidate may lose his opportunity to an ineligible candidate.

1.4 Objective

• To define a general schema and use cryptographic methods to create Digital Academic Certificates
• To build a secure, scalable blockchain-based storage system for storage of the digital certificates.
• To develop an interface for data custodian and data consumer to store, manage, and deploy data certificates and upload, Authenticate certificates respectively.

1.5 Description

The physical certificates are converted into digital records. These digital records are stored in a blockchain network. Where the records once stored are immutable and cannot be changed forever due to the smart contracts. These digital records are created by the institution (issuer) and are deployed on the blockchain. A Certificate Id is sent to the user that is student or holder of the certificate. This Id can be sent to anyone intended to check or Authenticate the digital certificate. For example, A company that is hiring the candidate and needs to verify the certificate authenticity of the candidate can verify it through our web application which is developed using MongoDB, React.JS, Node.JS, and Express.JS (MERN).

II. LITERATURE SURVEY

[1] Zibin Zheng et al. Blockchain as a Notarization Service for information Sharing with Personal data Store: Provides a blockchain-based design to produce the credibility verification of the shared documents in period whereas maintaining necessary privacy. Discusses usage of blockchain to realize Associate in Nursing audit path of the accesses to the shared data. Whereas keeping the audit path non-public to the people involved.

[2] Richard Nuetey et al. Block-certs and therefore the Digital Certificates project was undertaken at Media Labs Massachusetts Institute of Technology: An incubation project by the Media research laboratory Learning Initiative. Associate in Nursing the Learning Machine that builds a scheme for making, sharing, and validating bitcoin blockchain-based academic certificates. Digital certificates square measure registered on the Bitcoin blockchain, cryptographically signed, and tamper proof.

[3] Omar S Saleh et al. Authentication of User Details: The blockchain should certify users. during this case, the users square measure students, universities, institutes, employers, etc. every user in an exceedingly blockchain ledger are verified for accessing the certificate kept thereon. Authentication for users is thru a username and secret, or some system can even have multiple authentication systems like biometric, etc. as an example, the leader required to verify the certificate should initial be part of the blockchain and therefore the recipient can authorize the leader to look at the certificate and verify it.

[4] Omar S Saleh et al. The Project underneath taken by University of the capital of Cyprus: University of the capital of Cyprus (UNIC) is victimization the Bitcoin blockchain for several activities like acceptive bitcoin for tuition for any syllabus, issuance of educational certificates on Bitcoin blockchain, so on [26]. academic certificates within the blockchain initiated by the University of the capital of Cyprus is meant to eliminate fraud and conjointly overcome fraud in payments from international students. the most goal is to beat the issues of change of state with the numbers of student cohorts. UNIC has commenced issuance of all diplomas victimization the blockchain since 2017 and provides software package tools through that users will ensure the credibility of the certificate. the present ASCII text file standards square measure utilized in their user-facing systems and UNIC may be a part of the Block-certs association. The hash formula particularly, SHA-256 is employed for sharing certificates as a PDF file different entity. SHA-256 is employed for its ability to form a hash from the certificate, however, the reverse isn't potential. The credibility of the certificate is preserved by looking at the certificate's SHA-256 at intervals in the index document. If the code is matched, the certificate is authentic. Despite these options to preserve the privacy, ownership, and integrity of certificates, enhancements square measure required to in public validate the hash, this is often one demand to permit employers to look at the certificate. additionally, the recipient might not be ready to authorize a possible leader to verify the certificate victimization the hash.

[5] Omar S Saleh et al. certainty is another blockchain based mostly digital credentials verification platform: Smart certainty is developed to determine the credibility of educational credentials on a blockchain and to beat the matter of pretending certificates. good certainty makes use of cryptographical sign language of academic certificates to produce transparency within the case of enlisting. the scholar can share the hash with the possible leader to verify the certificate. However, within the case of hash or digitally signed certificate, it is often troublesome for a legitimate user to achieve access as a result of the pc accessing this information are often attacked by Associate in Nursing unwelcome person. Another issue during this application is that cryptography doesn't guarantee information security, and so the basic security measures should be enforced to protect against threats. At a similar time, cryptographically secured certificates in good certainty don't enable the certificates to be faked simply.

[6] Omar S Saleh et al. Records Keeper: Records Keeper is another blockchain-based mostly answer to verify educational certificates. With Records Keeper, academic institutes will issue certificates and supply a receipt to the user which might be shared with a 3rd party to prove the certificate is authentic. The receipt obtained from the scholar is employed by the third party to verify the certificate's credibility within the Record Keeper ledger. There don't seem to be several complications during this mechanism, however, the parties interested to look at the certificate within the Record Keeper blockchain should have possession rights. This amounts to a transfer of possession to the third party which can cause a change of state. this might work well on a non-public blockchain to make sure the safety of the certificate.

[7] A Gayatri et al. Jin-Chiou Cheng university 'Blockchain and good Contract for Digital Certificate: Jin-chiou developed a software package so as to avoid counterfeiting certificates. thanks to the dearth of Associate in Nursing anti-forge mechanism, the graduation certificate is to be solid. so, the decentralized application was designed to support Ethereum blockchain technology. First, generate the digital certificate for the paper certificate then hash worth created for the certificate is kept within the blockchain system. Even it wont to verify the credibility of the certificate it needed another scanning app to scan the certificate. The system saves on paper, stops document forgery. however, the QRCode should be scanned with a smartphone and an online association is needed.

[8] A Gayatri et al. Project done by Ze Wang et al: Ze Wang et al designed blockchain-based certificate transparency and revocation transparency system. during this system, the certificate authority (CA) signed the certificate, and therefore the revocation standing data of the revered certificates square measure revealed by the topic (Certificate Authority). Public logs square measure wont to monitor the CAs operation. this method was enforced with Firefox and nogix. this method provided the trust however Certificate validation is delayed and a false sense of security.

2.1 Existing System

If an organization is hiring an associate worker, they'll perform a background check. associate worker Background verification method could be a thorough screening of a candidate's work history within the past, education background and degrees, educational certificates, legal records, and most credit scores. the method sometimes takes between 3-10 days. This goes up just in case of intensive checks and for senior-level hires. Statistics show that almost all candidates aren't entirely truthful on their resumes and infrequently exaggerate their skills and talents. it's clear that education verification checks square measure essential build. employers make appropriate hiring choices. the corporate runs a background check on one's resume/CV, once all the interview rounds square measure qualified by the worker. an associate worker background check could be a review of a person's industrial, criminal, employment, and/or money records.

Many employers conduct background checks on job candidates through third-party corporations that verify the candidate's background by confirming with the past executive department or university and visiting home address to verify the residence. Some employers conduct checks when they need to be employed associate workers. large cash is spent by the corporate throughout this background verification method. So, there square measure tons of physical document checks while not knowing it's legit or authentic and it takes a large quantity of your time for verification. the most aim is to scale back of these large tasks and third-party involvement which can compromise the system to straightforward, direct, and secure interaction between an organization and also the candidate certificate.

2.2 Proposed System

Online Authentication of documents will reduce the investment of time during a background check. Since the world is getting digitized, the idea of online authentication of academic documents will help many students/institutes and also recruiters. In this model, the Admin/University will be responsible to upload the student's academic details into the blockchain using Dapp upon which a unique Certificate Id will be generated and the same will be sent to the respective student email. Now if the company is looking to hire an applicant. The student/applicant will have to share his/her unique Certificate Id with the recruiter, the same Id is used to view and verify the authenticity of a certificate. Since the Certificates are in blockchain, Data immutability and Security are strictly maintained. Overall, developing a Decentralized application that is universally accessible for students/employers to view and verify academic certificates without any third-party involvement, which is very simple to use, also efficient will make a major impact in near future.

III. TECHNOLOGIES USED

- **Ethereum**
  Ethereum is a global, open-source platform for decentralized applications. On Ethereum, you'll be able to write code that controls digital price, runs precisely as programmed, and is accessible anyplace within the world.

- **Ropsten Ethereum test Network**
  Ropsten is AN Ethereum testnet (or test network). Testnet are generally utilized by developers to run "tests" for his or her application or software system. Currency on testnet is worthless.

- **MongoDB Atlas**
  MongoDB Atlas is that the world cloud information service for contemporary applications. It provides availableness, measurability, and compliance with the foremost strict information security and privacy standards.

- **Truffle**
  • Built-in good contract compilation, linking, preparation, and binary management.
  • Automated contract testing for speedy development.
  • Network management for deploying to any variety of public & non-public networks.
  • Truffle documentation: https://www.trufflesuite.com/docs/truffle/overview

- **Web3.js**
  Web3.js could be an assortment of libraries that enable you to act with a neighborhood or remote Ethereum node, victimization, and protocol, or IPC association.

- **SendGrid: Email Delivery Service**
  SendGrid provides a cloud-based service that assists businesses with email delivery. The service manages varied varieties of email as well as shipping notifications, friend requests, sign-up confirmations, and email newsletters.

- **Infura**
  Infura provides the tools and infrastructure that enable developers to simply take their blockchain application from testing to scaled preparation - with easy, reliable access to Ethereum and IPFS.

IV. METHODOLOGY

• A digital certificate is essentially a JSON Object with the necessary fields needed for our cert-issuer code to place it on the blockchain. For which a hash can be generated and used for verification purposes.

• Blockchain storage methodology Ethereum is utilized to develop an architecture to store and manage digital certificates.

• Modern web development technologies such as React-js, Node-js are utilized to build an interface that facilitates the user to view, manage, and verify documents online.

4.1 ARCHITECTURE DIAGRAM

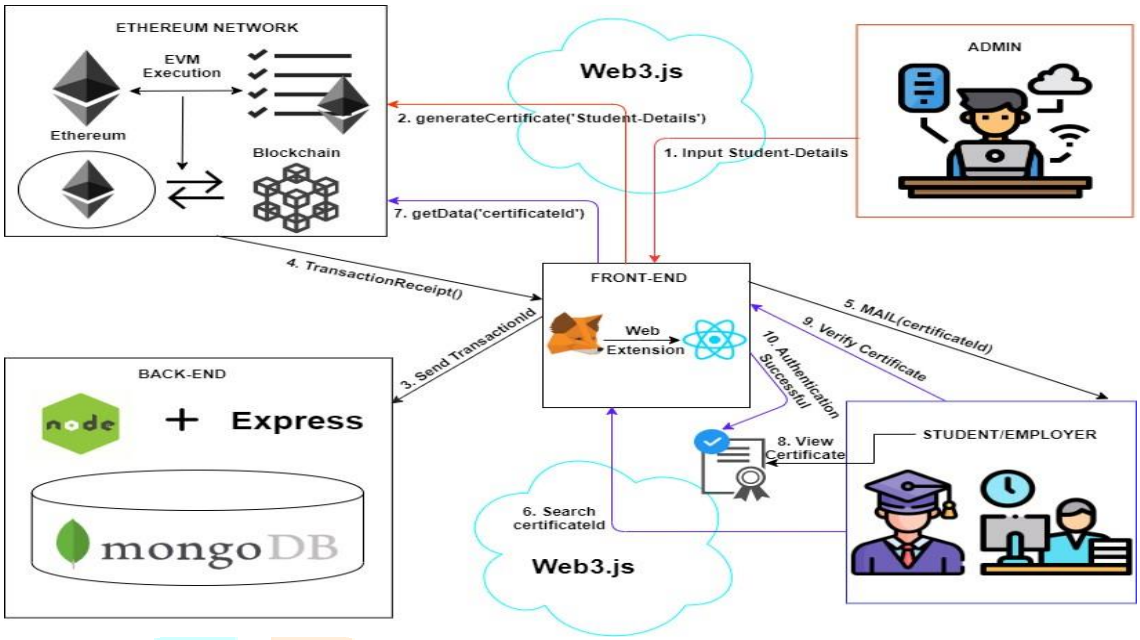

Figure 4.1 Architecture of Diagram.

A model may be a complete, basic, and simplified description of software system design that consists of multiple views from a selected perspective or viewpoint as shown in figure 4.1. A read maybe an illustration of a complete system from the attitude of a connected set of issues. it's accustomed to describe the system from the point of view of various stakeholders like end-users, developers, project managers, and testers.

4.2 USE CASE DIAGRAM

A use case diagram within the Unified Modelling Language (UML) may be a variety of behavioral diagrams outlined by and created from a Use-case analysis. A use case diagram may be an illustration of a user's interaction with the system that shows the connection between the user and therefore the totally different use cases within which the user is concerned. It will establish the various styles of users of a system and the totally different use cases and can usually be amid alternative styles of diagrams still. Use case diagrams area unit sometimes noted as behavior diagrams accustomed to describe a collection of actions that some system or systems ought to or will perform in collaboration with one or additional external users of the system (actors). Each use case ought to offer some evident and valuable results to the actors. Use case diagrams area unit, in reality, twofold - they're each behavior diagrams, because they describe the behavior of the system, and that they also are structure diagrams - as a special case of sophistication diagrams wherever classifiers area unit restricted to be either actors or use cases associated with one another with associations . The main purpose of a use case diagram is to indicate what system functions have performed that actor. Use Case diagrams area unit formally enclosed in two modelling languages outlined by the OMG: the Unified Modelling Language (UML) and therefore the Systems Modelling Language (SysML).

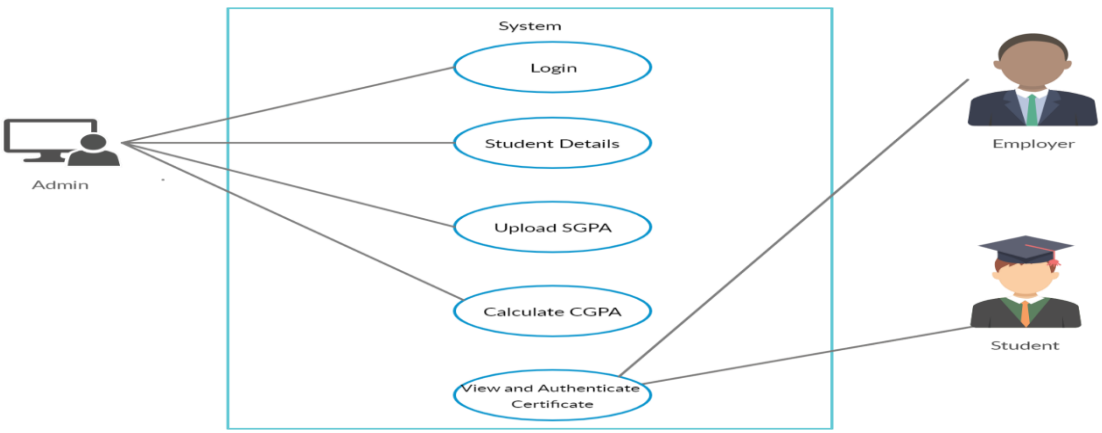

Figure 4.2 use case diagram

figure 4.2 shows the use case diagram of the "Blockchain-Based Academic Certificate Authentication System" in which admin/university can log in and generate a certificate based on student performance. Students will receive mail from the university which contains Certificate Id. With the help of Certificate Id students can view their certificate. If a student shares the Certificate Id with the employer, he can verify the authenticity of the certificate.

4.3 WORKFLOW

Step 1: Admin will fill student academic details in a form provided using Dapp interface.
Step 2: Admin submits the pre-viewed form details to Ropsten Blockchain Network
Step 3: When the certificate is uploaded into Blockchain. Certificate Id is generated and sent to respective student email.
Step 4: Students can share the Certificate Id for certificate verification.
Step 5: With the help of Dapp Interface Company HR can verify the certificate.
Step 6: Verification of Certificate Id query request will take place.
Step 7: Query result is displayed i.e., verified or failed.
Step 8: HR can confirm the certificate.
Step 9: The student will use his Certificate Id to view the certificate.
Step 10: Query request to search Certificate Id in the blockchain.
Step 11: Query result for the Certificate Id will be displayed.
Step 12: Students can view their Certificate (Verification of certificate is optional for student)

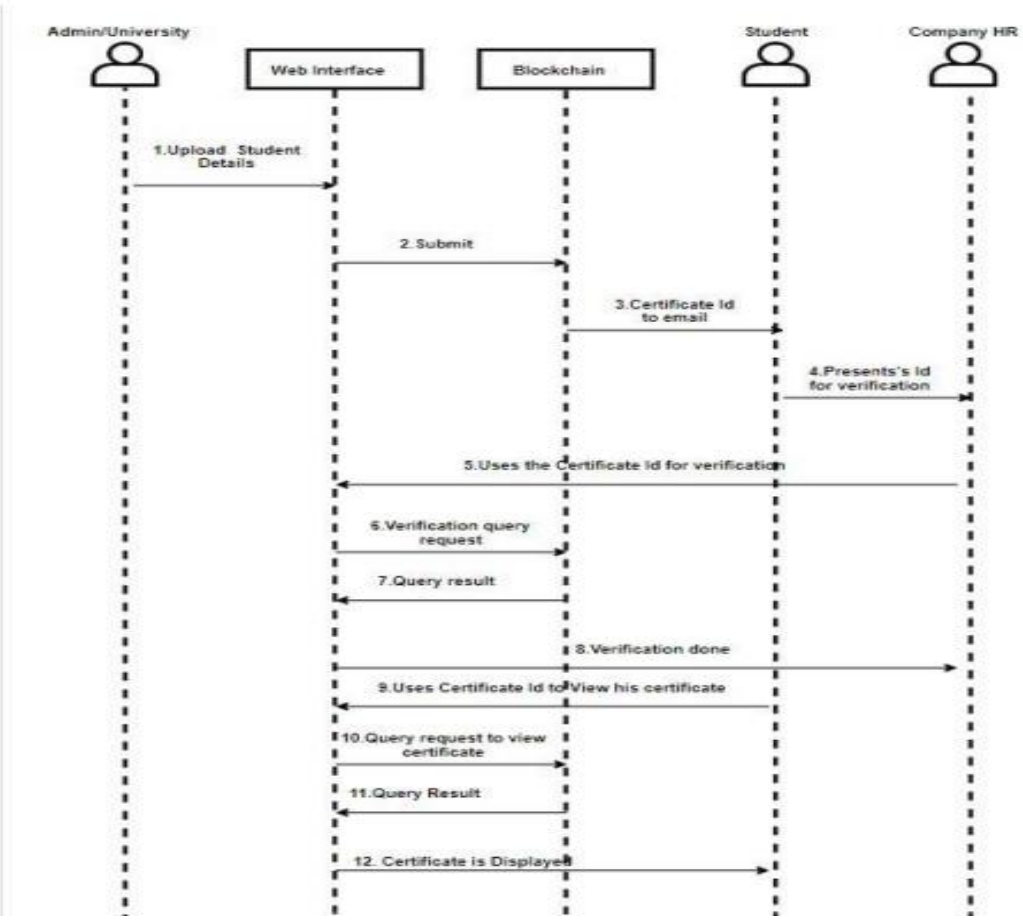

Figure 4.3 Workflow

4.4 SEQUENCE DIAGRAM

A sequence diagram in Unified Modelling Language (UML) can be an affordable interaction diagram that shows but processes operate with one another and in what order and at a specific time. it is a construct of a Message Sequence Chart. Sequence diagrams area unit usually called event diagrams, event scenarios, and temporal arrangement diagrams. figure 5.4 offers information regarding the sequence of operations.

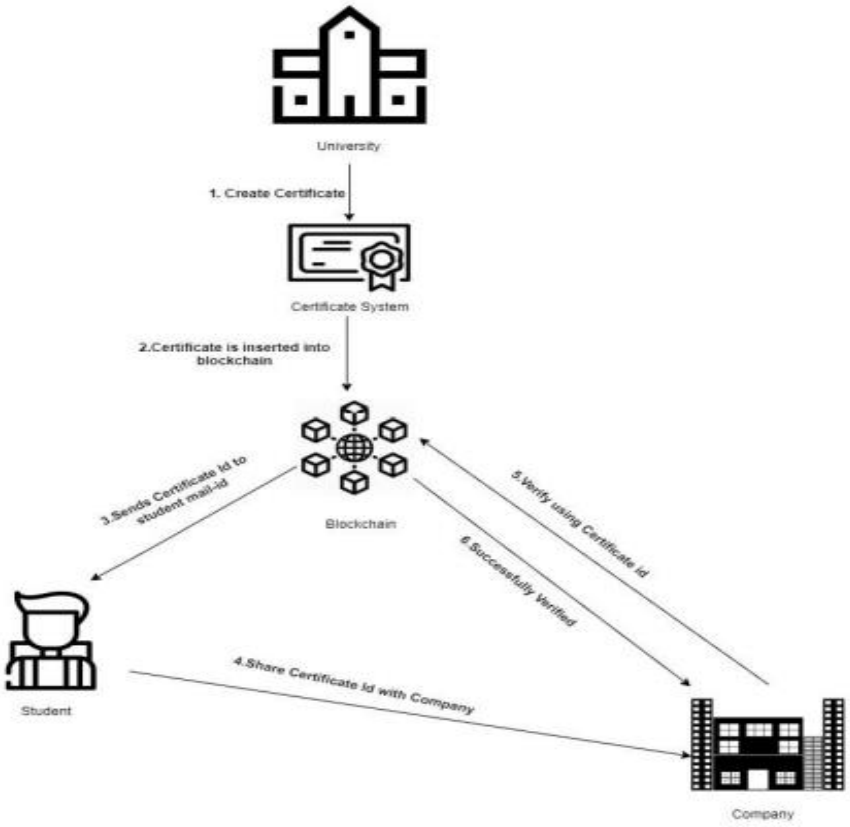

Figure 4.4 Sequence Diagram

V. APPLICATION

- Certificates are securely stored on Blockchain Network.
- Right person will get the Right Job Opportunity.
- Issues related to fake certificates will be avoided.
- Every time student needs to attest his/her certificate for the verification. This can be avoided.
- Certificates are easily accessible.
- Once the certificates are deployed on the Blockchain Network that will became Immutable. So , Certificate Data will not be altered.
- Manual Verification of the Certificate takes more time. This issue will be solved using Digital Certificate Verification System That will take very less time to verify Certificate.
- Blockchain Contains Distributed Database So Security level is high Compare to other technology.

VI. CONCLUSION

Despite thousands of job opportunities being created every year, many graduates end up without jobs, one of the reasons is the issue of fake certificates which Results in ineligible students getting jobs and other confidentiality issues. The System is designed in such a way that it removes the effect of fake certificates by introducing Digital Academic Certificates and providing a Highly secure Blockchain-Based storage architecture to store these certificates since data in a blockchain is immutable, the Authenticity of the Academic certificates is maintained and Web interface is developed to provide quick access to the Certificates and Authentication of the same.

REFERENCES

[1]. Zibin Zheng, Shaoan Xie, Hongning Dai, Xiangping Chen, and Huaimin Wang: An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends, 2017 IEEE 6th International Congress on Big Data.

[2]. Issuing and Verifying Digital Certificates with Blockchain : 2018 International Conference on Advanced Technologies for Communications - 978-1-5386-6542-8/18/$31.00 ©2018 IEEE.

[3]. Richard Nuetey Nortey , Li Yue, Promise Ricardo Agdedanu, Michael Adjeisah: Privacy Module for Distributed Electronic Health Records(EHRs) Using the Blockchain , 2019 the 4th IEEE International Conference on Big Data Analytics .

[4]. Mohammad Jabed Morshed Chowdhury, Alan Colman, Muhammad Ashad Kabir, Jun Han and Paul Sarda: Blockchain as a Notarization Service for Data Sharing with Personal Data Store, 12th IEEE International Conference on Big Data Science And Engineering.

[5]. Block certs A project undertaken at Media Labs MIT, Available at https://www.blockcerts.org.

[6]. National Academic Depository (NAD) a project undertaken by MHRD, India.

[7]. Blockchain Based Framework For Educational Certificates Verification : Journal of critical reviews ISSN- 2394-5125 Vol 7, Issue 3, 2020.

[8]. Certificate validation using blockchain : IEEE 7th International Conference on Smart Structures and Systems ICSSS 2020-978-1-7281-7223-1/20/$31.00 ©2020 IEEE