# Verification of Digital Certificate using Blockchain

Prof. Roshni Narkhede[1], Nikhil Rananaware[2], Kunal Kale[3], Aditya Gadhave[4] Department of Computer Engineering [1,2,3,4]
Nutan Maharashtra Institute of Engineering and Technology, Pune, Maharashtra [1,2,3,4 ]

**Abstract -** An algorithm for blockchain technology is described in this article to validate digital certificates. Graduation certificates must be easily validated because the number of students and graduates from universities and other higher education institutions is increasing annualy[1]. In this research, we propose two financial models where employers and graduates are the primary service players and the price of services is balanced. Employers want quick and dependable verification of their employees' degrees, and students want inexpensive, easily verifiable certificates. False credentials are a serious problem. It's not hard to obtain a phony education certificate in India. Employers who take on thousands of first-year students pay a large sum of money to have the qualifications and academic records of candidates verified.

***Key Words*:** (Blockchain, Document Verification, Digital Certificate, distributed, Pre-processing).

## 1. INTRODUCTION

Students will receive numerous certifications during the session. These credentials are presented by students when they seek for jobs in the public or private sectors. It is necessary to personally verify each of these certifications[3]. There are instances when students offer phony credentials that are hard to spot. In academia, the problem of phony academic credentials has long existed. This is due to the fact that these certificates are inexpensive to create and necessitate manual validation, which makes the validation procedure extremely difficult. By keeping digital certificates on the blockchain, this issue can be resolved.

### 1.1 Problem Definition

The issue of fraudulent certificates in current systems is a significant one. Businesses that hire thousands of new hires make a substantial financial commitement in confirming the qualifications and educational background of applicants[1]. We are utilizing blockchain technology to validate educational certificates through the implementation of a system of electronic system in order to address this problem.

### 1.2 Model Architecture

Universities must first enroll in order to receive blockchain-based unchangeable credentials. Every university has a wallet address that can be used to send money. Owners of smart contracts are the only ones who can add universities. The university can use the system to create document with data domains once it has been uploaded.[14] Every created certificate is returned with a distinct hash produced by the SHA-256 method and saved in the Interplanetary File System (IPFS). This functions as a special ID for every document [15]. The learner receives the transaction ID that results from storing all of this information on the blockchain, together with the hash and certificate details that were generated.

.

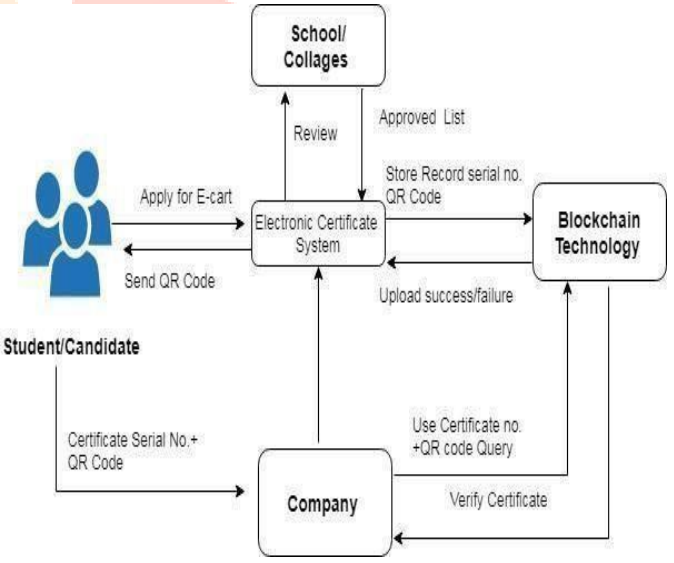


**Fig.1: Model Architecture**

### 1.3 Shamir Secret Sharing

A strategy for sharing a particular secret share among a number of reliable participants is known as a secret sharing scheme in cryptography. You ought to keep this information private and safe even though it can contain really crucial information that you'll need later.[13] As a combination, these stocks illustrate and rebuild the riddle, but individually they are completely worthless. Consider a secret sharing program that is similar to a jigsaw puzzle as a brainstorming exercise[10].

where the ten players each receive a portion of the problem, but it is entirely blank. Only when all the pieces are assembled will the puzzle's image become apparent.[4] To breach the system, the idea is to disperse keys from one physical location to several different sites.

.

### 1.4 SHA-1(Hash)

From an input, the cryptographic hash function and the hash result generated by algorithm is 160 bits [5].For this message digest, a 40- digit hexadecimal number is often displayed[7]. This federal information processing standard was produced by the US National Security Agency. SHA-1 has been seen as unreliable since 2005. Major IT firms like Google, Apple, Microsoft, and Mozilla ceased supporting SHA-1 in 2017.

## 2. Objectives

In addition to saving paper, the system lowers administrative expenses, stops document forgeries, and offers accurate and trustworthy digital certificate information[8]. The correctness, security, and immutability of the data are guaranteed by this system. Develop a validation algorithm that is capable of verifying every peer for every request for access.

## 3. Scope of Study

Boxes in class diagrams stand in for classes. A class diagram is a kind of structural diagram that uses the classes, properties, operations, and relationships between classes to illustrate a system's structure.In [3] Representing a system's static structure in terms of classes and the connections between them is the aim of a class diagram.

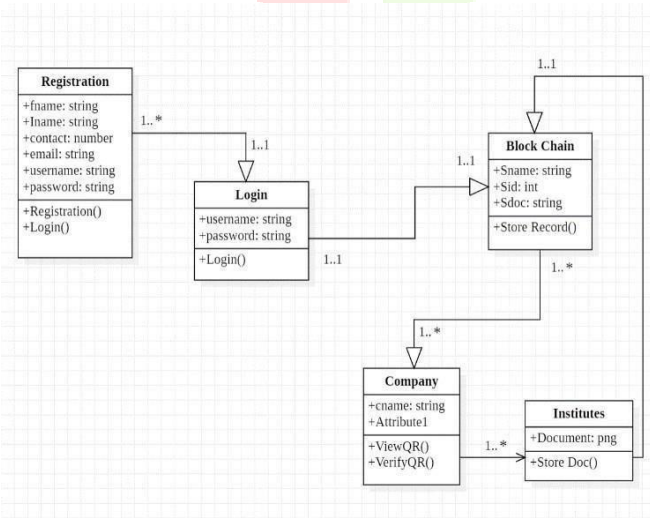


**Fig .2: Class Diagram**

Activity diagrams are graphical representations of step-by-step activity and action workflows that support selection, repetition, and concurrent execution.[10]Activity diagramscan be used to illustrate the dynamic aspects of a system. A flow chart showing the flow from one activity to the next. Activity diagrams are therefore considered flowcharts.[4] The main element used in this diagram is the activity itself. Activities are functions performed by the system. Activity diagrams are good for modeling the activity flow of a system.

.

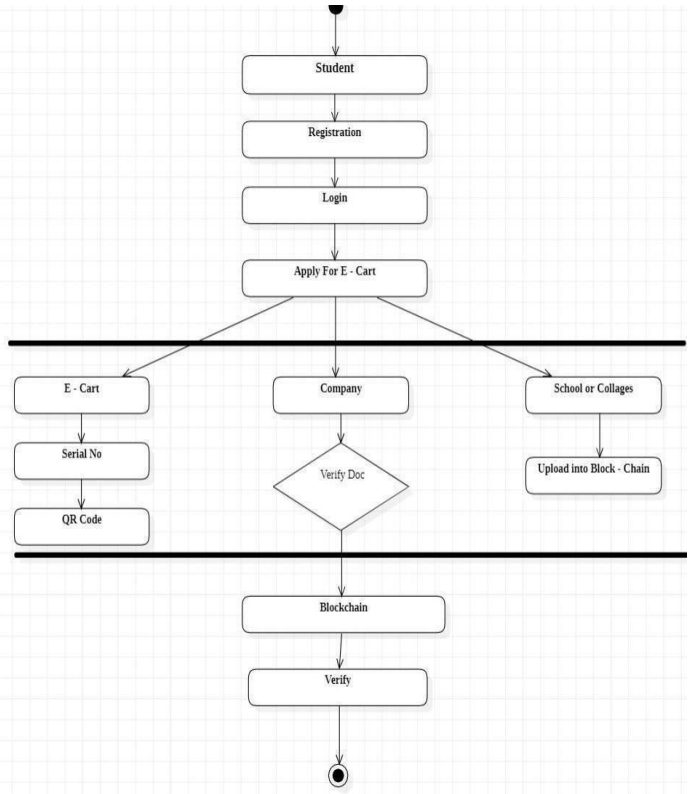


**Fig .3: Activity Diagram**

A use case diagram outlines the system's scope and high-level capabilities. Use case illustrations illustrate how system users of the system under design interact with other people or external devices.[5] Use cases for suggested system requests are frequently created in conjunction with software developers and other users.

.

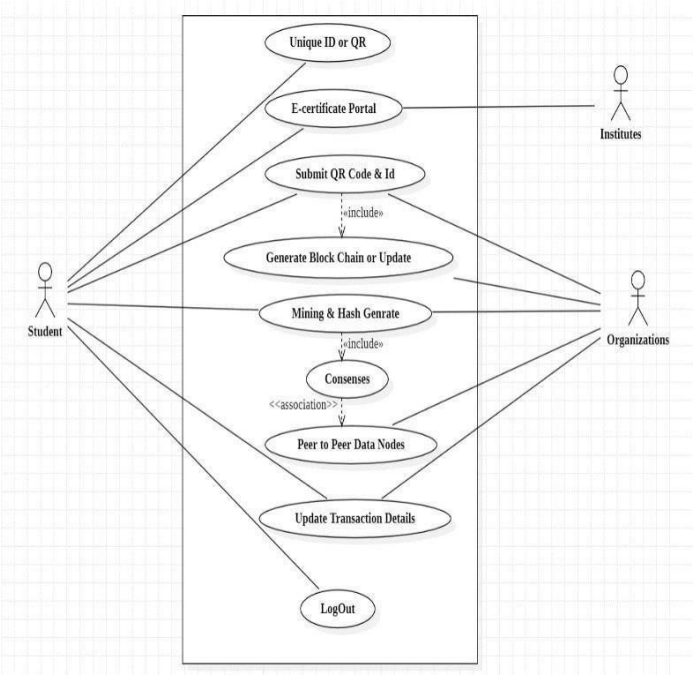


**Fig .4: Use Case Diagram**

## 4. CONCLUSIONS

We have effectively examined the operation of digital certificate validation in this study. When implementing candidate validation in a corporate setting and using legally certified candidate certificates, this paradigm can be applied. Within the system, the automatic issuing of certificates is transparent and open[11]. As a result, an organization or business can ask the system for information regarding certificates. In addition to preventing document forgeries and saving administrative costs, the suggested solution offers accurate and trustworthy digital certificate information.

.

## ACKNOWLEDGEMENT

This document is supported by NMIET,Pune(410507) We would like to express our sincere gratitude to everyone who gave us valuable opinions toward the completion of the seminar report of "Document verification & Validation Using Blockchain", which is part of the curriculum of this seminar. We thank the cooperating departments for providing valuable support and prerequisites for system development. We are very grateful to Professor Roshani Narkhede for guiding us in the right way, giving her time whenever needed, giving her knowledge and sharing their experience in carrying out this project. We would like to thank you for correcting our doubts by providing them.

## REFERENCES

[1] "Blockchain and Smart Contract for Digital Certificate, "by Jiin-Chiou Chen, Yi-Hua Chen, Chien Chi, and Narn – Yih Lee Applied System Innovation Proceedings of the 2018 IEEE International Conference 2018 IEEE ICASI- Meen, Prior, & Lam(Eds).

[2] "Security Applications and Challenges in Blockchain ," by Austin Draper, Aryan Familrouhani, Devin Cao, Tevisophea Heng, and Wenlin Han Presented at the 2019 IEEE International Conference on Consumer Electroniccs(ICCE).

[3] Giuseppe Gottardi, Emanuele Fronttoni, Marco Baldi, Daniele Sciarroni, Luca Spalazzi, and Franco Chiaraluce At the first Italian Conference on Cybersecurity(ITASEC17) Proceedings, a certificate titled " Validation through Public Ledgers and Blockchains" was presented.

[4] Neethu Gopal, Vani V Prakash "Survey on Blockchain Based Digital Certificate System" International Research Journal of Engineering and Technology (IRJET) Nov 2018 SIGIR Conference on Research and Development in Information Retrieval, Santiago, Chile ,2015: 959-962.

[5] Glaser, F., & Bezzenberger, L. (2015). Beyond Cryptocurrencies - A Taxonomy of DecentralizedConsensus Systems. In European Conference on Information Systems

[6] Pazaitis, A., De Filippi, P. and Kostakis, V. (2017). Blockchain and Value Systems in the Sharing Economy: TheIllustrative Case of Back feed. Working Papers in Technology Governance and Economic Dynamics.

[7] A. Dorri, S. S. Kanhere, and R. Jurdak, "Blockchainin internet of things: Challenges and Solutions,"arXiv:1608.05187 [cs], 2016. [Online].Available:http://arxiv.org/abs/1608.05187

[8] An access control mechanism for cloud storage based on blockchain technology. Young Researchers in Electrical and Electronic Engineering.

[9] Decentralized PolicyHiding Attribute-Based Encryption with Receiver Privacy, Michalevsky Y, Joye M.

[10]] Maharshi Shah, Priyanka Kumar, "Tamper Proof Birth Certificate Using Blockchain Technology", International Journal of Recent Technology and Engineering (IJRTE), Volume-7, Issue-5S3, February 2019.

[11] " Blockchain and Smart Contract for Digital Certificate," edited by Jin-Chiou, Narn –Yih Lee, Chien Chi, and YI-Hua Chen, was published in IEEE International Conference on applied System Innovation 2018 proceedings.

[12] In the International Journal of Recent Technology and Engineering(IJRTE), Volume-7, Issue -5S3, February 2019, Maharashtra and Priyanka Kumar write about using blockchain technology to create tamper proof birth certificates.

[13] Emmanuel Nyaletey, Reza M. Parizi, Qi Zhang, Kim- Kwang Raymond Choo, "BlockIPFS - Blockchain- enabled Interplanetary File System for Forensic and Trusted Data Traceability", IEEE International Conference on Blockchain, 2019.

[14] "Blockchain Based Identity Verification Model", International Conference on Vision Towards Emerging Trends in Communication and Networking (ViTECoN), 2019, Gunit Malik, Kshitij Parasrampuria, Sai Prasanth Reddy, Dr. Seema Shah.

[15] In 2015 Glaser, F., & Bezzenberger, L published a paper. A classification of Decentralized Consensus system: Moving Beyond Cryptocurrencies . At the European Comference on Information Systems.