Digital Certificate Verification using Blockchain

Prof. Priyanka Abhale[1], Anjali Chikate[2], Shubhada Jadhav[3], Irshad Shaikh[4], Rutuja Bhole[5]

ALARD COLLEGE OF ENGINEERING & MANAGEMENT (ALARD Knowledge Park, Survey No. 50, Marunji, Near Rajiv Gandhi IT Park, Hinjewadi, Pune-411057) Approved by AICTE. Recognized by DTE. NAAC Accredited. Affiliated to SPPU (Pune University).

Abstract -This article describes a blockchain technology algorithm for validating digital certificates. As the number of university and higher education students and graduates continues to grow each year, there is a need to easily validate graduation certificates. In this paper, we project two financial models in which the price of services is balanced between graduates and employers as the main actors of services. Students demand cheap and easily verifiable certificates, and employers demand fast and reliable proof of their degrees. The issue of fake credentials is a big one. Getting a fake education certificate in India is not that difficult. Companies that hire thousands of freshmen spend a lot of money verifying applicants' educational credentials and qualifications. A blockchain is a distributed digital ledger collectively managed by a network of computers called nodes. Data on the blockchain cannot be changed by one person without the consent of everyone else holding the record. This keeps your data safe.

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

1. INTRODUCTION

During the training students will get many certificates. Students produce these certificates when applying for public or private sector jobs. All of these certificates must be manually verified. Sometimes students present fake certificates and are difficult to identify. The issue of fake academic credentials has long been a problem in academia. This is because such certificates are cheap to produce and require manual validation, which greatly complicates the validation process. This problem can be solved by storing digital certificates on the blockchain.

1.1 Problem Definition

In existing systems, the problem of fake certificates is a big one. Companies that hire thousands of freshers spend a lot of money verifying applicants' educational credentials and qualifications. To address this issue, we are implementing an electronic certificate system for validating educational certificates using blockchain technology.

1.2 Model Architecture

For blockchain-based immutable certificates, universities must first enroll. Each university has a wallet address for sending transactions. Universities can only be added by smart contract owners. Once added, the university can access the system to create certificates containing data fields. Each certificate created is stored in the Interplanetary File System (IPFS) and returned with a unique hash generated using the SHA-256 algorithm. This serves as a unique ID for each document. All this data, along with this generated hash and certificate details, is stored on the blockchain and the resulting transaction ID is sent to the student.

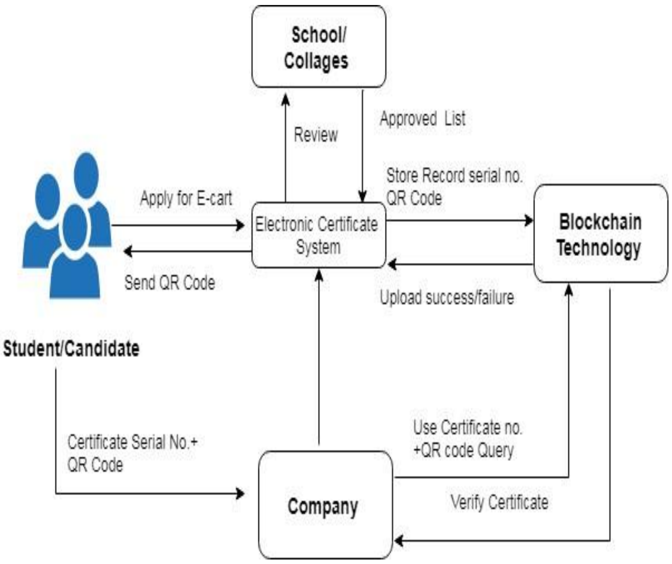

Fig -1: Model Architecture

1.3 Shamir Secret Sharing

In cryptography, a secret sharing scheme is a scheme of sharing a specific secret share between a group of trusted participants. This secret can be very important information that you may need in the future, but you should keep it private and secure. These stocks are utterly useless on their own, but when combined they reconstruct and visualize the mystery. As a thought experiment; think of a secret sharing program like a jigsaw puzzle where the pieces of the puzzle are divided among her ten players but completely blank. The image created by the puzzle is visible only when all the pieces are put together. The goal is to distribute keys from one geographic location to multiple locations in order to compromise the system.

1.4 SHA-1(Hash)

SHA-1, or Secure Hash Algorithm 1, is a cryptographic hash function that takes an input and produces a 160-bit (20-byte) hash value. This hash value is called the message digest. This message digest is typically displayed as a 40-digit hexadecimal number. It is a US federal information processing standard and was developed by the US National Security Agency. SHA-1 has been considered insecure since 2005. Browsers from major technology companies such as Microsoft, Google, Apple, and Mozilla stopped accepting SHA-1 SSL certificates in 2017.

2. Objectives

The system saves paper, reduces administrative costs, prevents document counterfeiting, and provides accurate and reliable digital certificate information. This system ensures the accuracy, security and immutability of information. Implement a validation algorithm that can validate each peer for each access request.

3. Scope of Study

Classes in class diagrams are represented by boxes. A class diagram is a type of structural diagram that describes the structure of a system by showing the classes, attributes, operations, and relationships between classes. The purpose of a class diagram is to represent the static structure of a system in terms of classes and the relationships between those classes.

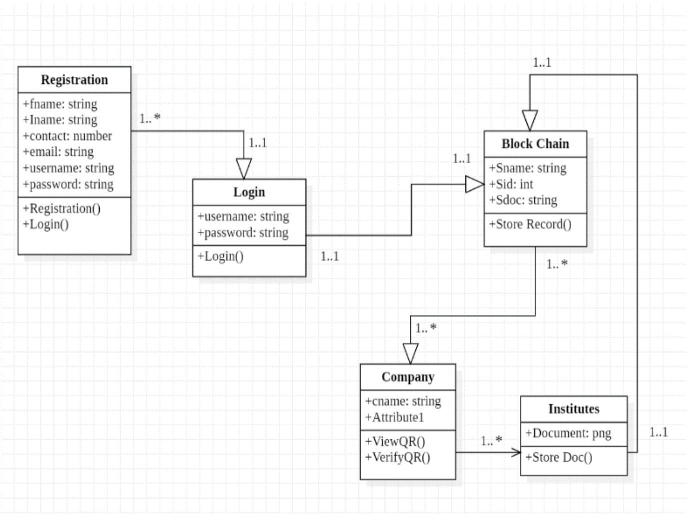

Fig -2: Class Diagram

Activity diagrams are graphical representations of step-by-step activity and action workflows that support selection, repetition, and concurrent execution. Activity diagrams can 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. 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.

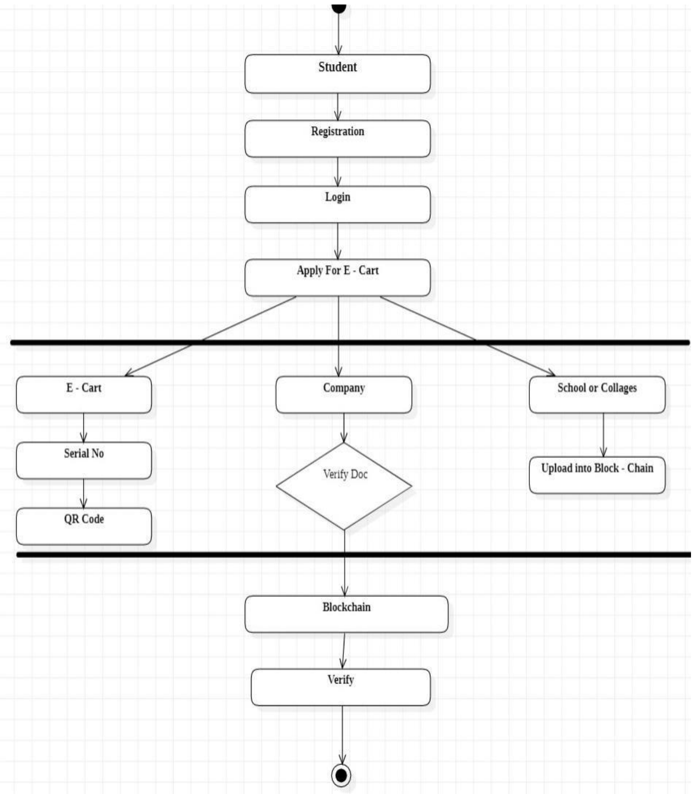

Fig -3: Activity Diagram

A use case diagram describes the high-level functionality and scope of the system. Use case diagrams describe interactions between Persons or external devices and the system under design. Use cases are often developed in collaboration with software developers and other users of the proposed system request. A use case diagram shows the relationship between actors and use cases.

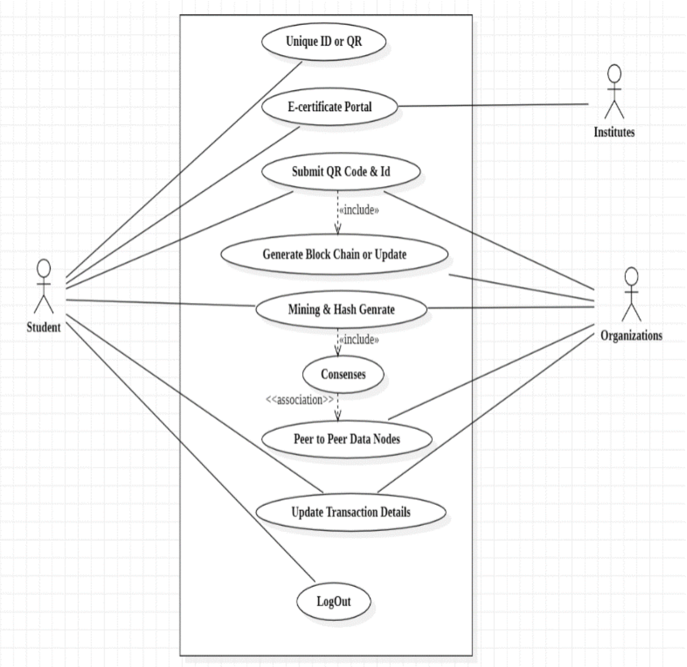

Fig -4: Use Case Diagram

4. CONCLUSIONS

In this research, we have successfully investigated how digital certificate validation works. This model can be used in enterprise implementations of candidate validation where candidate certificates are legally validated. The automatic certificate issuance is open and transparent within the system. Therefore, a company or organization can request information about certificates from the system. The proposed system saves administrative costs, prevents document forgery, and provides accurate and reliable digital certificate information.

ACKNOWLEDGEMENT

This document was supported by Alard College of Engineering & Management, Pune 411057. We would like to express our sincere gratitude to everyone who gave us valuable opinions toward the completion of the seminar report of "Digital Qualification Examination by 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 Priyanka Abhale 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] Jiin-Chiou Chen, Narn-Yih Lee, Chien Chi, and Yi-Hua Chen "Blockchain and Smart Contract for Digital Certificate" Proceedings of IEEE International Conference on Applied System Innovation 2018 IEEE ICASI 2018- Meen, Prior & Lam (Eds)

[2] Austin Draper, Aryan Familrouhani, Devin Cao, Tevisophea Heng, Wenlin Han "Security Applications and Challenges in Blockchain" Published in IEEE International Conference on Consumer Electronics (ICCE) 2019

[3] Marco Baldi, Franco Chiaraluce, Emanuele Frontoni, Giuseppe Gottardi, Daniele Sciarroni and Luca Spalazzi Certificate "Validation through Public Ledgers and Blockchains" In Proceedings of the First Italian Conference on Cybersecurity (ITASEC17) 2017

[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 Decentralized Consensus 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