Ethereum Decentralized Application for Storing Student Results

Avadhoot Bhogil[1], Vishal Bambare[2], Prajyot Chemburkar[3], Yogesh Shahare[4]

[1,2,3]B.E. Student, Department of Information Technology, MGMCET, Kamothe
[4]Professor, Mahatma Gandhi Mission's College of Engineering and Technology Kamothe, Maharashtra, India

---

Abstract - *A blockchain is a growing list of records, called blocks, that are linked together using cryptography. It's also described as a "trustless and fully decentralized peer-to-peer immutable data storage" that is spread over a network of participants often referred to as nodes. Each block contains a cryptographic hash of the previous block, a timestamp, and transaction data generally represented as a Merkle tree. In today's world, people can easily manipulate digital data as per their needs. One such example would be the manipulation of academic results by entities that may profit by exploiting students. A good solution to avoid such suspicious manipulation of data would be to develop a Decentralized Application based on Blockchain so that the manipulation of data becomes impossible. As a mark of certainty, the data can also be signed using PGP, so that Institutes, Corporations, or Universities can verify it for its legitimacy.*

Key Words: Blockchain, ERC20, Smart Contracts, Truffle, Metamask, PGP

1. INTRODUCTION

Diploma & degree certificates, internship & training certificates, Leaving certificates, Bonafide certificate, Domicile, Passing certificate, Character certificate, Letter of recommendation are some of the most important documents that an individual will require for their entire lifetime. Verification of these credentials is a fundamental process of an academic environment, and also plays an indispensable role for higher education and company placement drives.

To ensure the legitimacy of these issued documents, educational universities adopt various methods such as allocating unique identification numbers, appending students details like their date of birth along with a passport size photograph, distinctive hologram, etc. Furthermore, companies also need to verify the validity of these documents that they acquire from the students. This process is monotonous, expensive, and cumbersome.

1.1 Existing System

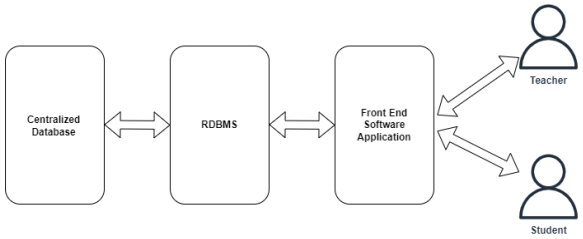

Fig-1: Existing Methodology

The traditional system involves the use of the Relational Database Management System (RDBMS) which uses a client-server architecture for serving information. In this system, the information can be modified by the client entity. A delegated authority has control over the database. Administration and maintenance of the database are carried out by this delegated authority. Before retrieving any information the client must authenticate itself. Speaking in the context of educational institutions, these records of grades should be immutable. Once a student has been graded the data should be saved and the database should not allow any further manipulations. Refer to Fig-1 for more clarity.

Let's take an example of a grade management system in any standard educational institution where teachers upload excel or CSV files on the platform or enter the grades manually. The platform uses a database that is managed by the institute's system administrator.

There are several disadvantages to this platform:

- Malicious actors can steal the credentials, and manipulate the database.
- Since the database is centralized the system administrator needs to be trusted.
- Both students and teachers have a common entry point to the platform

1.2 Proposed System

The architecture identifies 3 entities that have various functionalities:

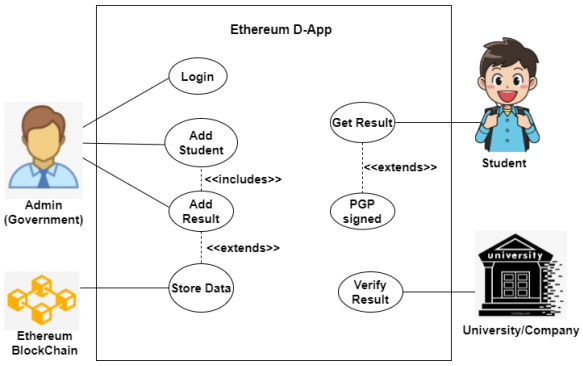

Fig -2: Use Case Diagram

a. Admin (Government):

- **Registration of Student:** Admin will add the student' data which in turn creates a unique ID for them
- **Adding Student Result:** Adding grades for different subjects which gets tallied to generate the final result
- **Signing Result:** The Result is automatically signed using a PGP key for certifying its legitimacy

b. Student:

- **View and Download:** The student is given only read permissions for the Result object which is downloadable in PDF format. The result will be displayed only if they provide correct credentials (Mothers Name and Registration Number)

c. University/Company/Employer:

- **Verification:** This Entity can verify the result which has been sent to them by the students, using the PGP signature.

Refer to Fig-2 for more clarity.

To develop a prototype of the proposed architecture we make use of the following technologies:

a. Ethereum Smart contract:

From ethereum.org, "*A smart contract is simply a program that runs on the Ethereum blockchain. It's a collection of code (its functions) and data (its state) that resides at a specific address on the Ethereum blockchain.*"

Smart contracts in Ethereum are a type of account that can carry out transactions over a blockchain network but are not operated by a user. Instead, they act upon a pre-written code and its functions. They are written in Solidity.

We will be deploying smart contracts to automatically append, and fetch students' data and their results on the blockchain.

b. Truffle framework

From trufflesuite.com, "*Truffle suite is a world-class development environment, testing framework and asset pipeline for blockchains using the Ethereum Virtual Machine (EVM), aiming to make life as a developer easier*"

Truffle is used to create a Development Environment for Ethereum Projects. Ganache, a tool in the Truffle framework, allows creating a blockchain on the local system with multiple test accounts.

c. Metamask

From metamask.io, "*MetaMask provides the simplest yet most secure way to connect to blockchain-based applications. You are always in control when interacting on the new decentralized web.*"

Metamask provides passwords and keys for setting up a crypto wallet, also taking care of privacy and security

d. PGP

From wikipedia, "*Pretty Good Privacy is an encryption program that provides cryptographic privacy and authentication for data communication*"

PGP can be used for data verification by signing said data with a PGP Private Key. Data can be verified by decryption with a public key.

This process will be used by Employers, Universities, or Companies to verify the results that have been sent to them.

2. Implementation

The data flow begins with Admin, who will add student information including Student Name, Mother's Name, Student ID, DOB, Hall ticket Number, and Optional Subject. The Admin will also add the student's marks. The Smart Contract now will calculate the gas fee for this transaction and let Metamask know. The Admin will confirm the

transaction via Metamask which pushes the data onto the blockchain. The data will be saved as a newly mined block onto the chain.

Now that the data is securely stored on the blockchain it can be downloaded by students. Students will be able to download results by providing their Student ID (Hall Ticket), and Mothers Name. The result is now available to the students in pdf format that is signed with PGP.

The Students may now send these results to universities or companies as part of their CV. The companies can easily verify the legitimacy of the result by using the PGP signature.

Refer to Fig-3 for more clarity:

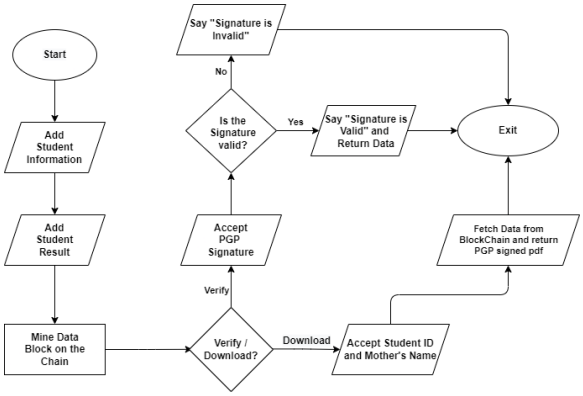

Fig-3: System Architecture Diagram

3. Experiment Results

The developed DApp is deployed over Ganache. Table 1 shows the deployment cost of smart contracts. The Student Smart Contract contains rules for deploying both student data and the results onto the blockchain.

Table 1: Deployment Cost of Smart Contracts

Contract Name	Deployment Cost (Gas Fee)
Migration (Default Ethereum Contract)	202155
Student	985578

Table 2 shows the Transaction cost to push data onto the blockchain. It is the amount of Ethereum (Gas Fee) that is transferred to the Smart Contract account.

Table 2: Transaction Cost of adding data

Transaction Type	Transaction Cost (Gas Fee)
Student	42251

4. Conclusions

The Paper shows an effortless and practical blockchain-based architecture for storing and retrieving students' results.

The Decentralized Application is developed and its execution is analyzed in terms of transaction and deployment cost.

5. Future Vision

In the future, we plan to increase scalability and standardize the platform so that different Grading formats can be assessed. We plan to test our prototype with other universities connecting them in one private blockchain

References

[1] Dezhi Han, "A Blockchain-Based Educational Records Secure Storage and Sharing Scheme", IEEE, Volume 7, November 2019.

[2] Raaj Anand Mishra, Anshuman Kalla, Nimer Amol Singh, Madhusanka Liyanage, "Implementation and Analysis of Blockchain Based DApp for Secure Sharing of Students' Credentials", IEEE Consumer Communications & Networking, March 2020.

[3] Emanuel Bessa, Joberto Martins, "A Blockchain-based Educational Record Repository", HAL, 31 Mar 2019.

[4] Prof. Luca Ardito, prof. Maurizio Morisio, "Blockchain based storage of students career", POLITECNICO DI TORINO, December 2018.

[5] Rushikesh Pawar, Sambhaji Jadhav, Sainath Rodge, "Secured University Results System using BlockChain Features", International Journal of Research in Engineering, Science and Management, Volume 2, May 2019.

[6] Lindsay Marshall, Ellis Solaiman, Bakri Awaji, "Blockchain-Based Trusted Achievement Record System Design", International Conference on Information and Education Innovations, August 2020.

[7] Zibin Zheng; Shaoan Xie; Hongning Dai; Xiangping Chen; Huaimin Wang, "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends", 2017 IEEE International Congress on Big Data (BigData Congress), September 2017.

[8] Dejan Vujičić; Dijana Jagodić; Siniša Ranđić, "Blockchain technology, bitcoin, and Ethereum: A brief overview", 17th International Symposium INFOTEH-JAHORINA (INFOTEH), April 2018.

[9] Kevin Delmolino, Mitchell Arnett, Ahmed Kosba, Alexandria University, Andrew Miller, "Step by Step Towards Creating a Safe Smart Contract: Lessons and Insights from a Cryptocurrency Lab", International Conference on Financial Cryptography and Data Security, February 2016.

[10] Alex Roehrs, Cristiano André da Costa, Rodrigo Da Rosa Righi, "A Distributed Architecture Model to Integrate Personal Health Records", Journal of Biomedical Informatics, Volume 71, May 2017

BIOGRAPHIES

Avadhoot Shivaji Bhogil
BE-IT MGMCET (Final Year)

Prajyot Manish Chemburkar
BE-IT MGMCET (Final Year)

Vishal Vidyadhar Bambare
BE-IT MGMCET (Final Year)

Yogesh Shahare
Assistant Professor MGMCET