International Journal of Advanced Science and Technology
Vol. 29, No. 5, (2020), pp. 4244 - 4254

Academic Credential Verification Technique Using Blockchain

Anant Shukla[1], Sneha Indra[2], Tanisha J Trivedi[3], Ujjwala Singh[4]
under the guidance of Ms Monica Catherine[5]

Department of Information Technology, SRM Institute of Science and Technology
[1] *as4698@srmist.edu.in,* [2]*si9205@srmist.edu.in,* [3]*tt9552@srmist.edu.in,*
[4]*us3218@srmist.edu.in,* [5]*monicacs@srmist.edu.in*

Abstract

Academic credentials are highly crucial for an individual. With the help of it, one's academic progress is determined. Whether it is to apply for a job, higher education, applying for a passport or visa, academic credentials are one of the essential documents.

But nowadays, fake academic credentials can be created and hence verification of the credential by the issuer is mandatory. Verification of academic credentials involve both the candidate and the certificate issuer and takes days or weeks to verify the submitted credential. Hence, employers/ institutions and candidates need to spend their valuable time for each request.

Saving the digital certificates on the Blockchain solves this problem. The Blockchain platform allows transactions to be immutable and openly verifiable; these Blockchain assets are used for building digital certificates, which are convenient to validate and anti-counterfeit.

Keywords: *Blockchain, Decentralization, Ethereum, Academic Credential Verification, Smart Contract*

1. Introduction

During our research, we realised the need for a verification portal for verifying the academic credentials of students who have graduated from a particular college. The academic progress is determined by evaluating the marks, and the percentage one has gained. We can see this when we apply for jobs or even colleges for higher studies. Academic transcripts are one of the essential documents they want. In most of the universities, these credentials are given in the form of hard copies to students.

For verification of the credentials, the organisation has to manually examine all the data which makes the system very time-consuming.

Also, there is always a possibility that some may produce fake academic credentials which may also get unnoticed.

We solved the problem of manual verification of each certificate and also eliminated situations where students use forged data by storing the digital certificates on the Blockchain. Blockchain is a decentralised shared distributed ledger. No modification to the data held in Blockchain is possible; and if any data is modified, it can come into immediate notice, preventing it from being propagated to the public ledger.

In this study, we have developed a decentralised web application which uses Blockchain to store the academic credentials of all the students who have graduated from the University. This Decentralised application is written in Solidity and uses the Ethereum Blockchain technology.

ISSN: 2005-4238 IJAST

2. Current Methodology

Currently, credential verification involves manual verification by the organisation.

Verification of academic credentials involves the authority requiring the verification, student and the certificate issuer. The manual confirmation by the college can have errors, and there is a chance of forgery. The verification process can take several weeks to be processed and hence employers/ institutions; candidates need to spend their valuable time for each request. This reduces the efficiency of the system. An example of the system followed in our University is:

Any requests for verifications are sent to the HoD who forwards these to the concerned faculty in-charge who forwards these requests to the COE office where the certificates are verified and sent back to the faculty in-charge, who sends them back to the HoD who contacts the institution with the verification status.

This makes the whole process tedious and time-consuming. Any delay in the process chain affects the entire process, which may have adverse consequences for the student.

3. Tools Used

3.1 Blockchain

In 2008, an individual named Satoshi Nakamoto introduced the concept of Blockchain.

This is a decentralized public ledger controlled by the rules where each node participating in the blockchain network maintains a database of all the data in the network. The records of several transactions are preserved in blocks along with their time stamp, and each transaction should be checked independently by utilizing the hash value because it is accessible, widely verifiable and the records entered cannot be changed, thus avoid forgery. In Blockchain the hash value of the preceding block connects each series of transactions to the preceding series. So, if someone wants to alter any data in the Blockchain, the block's hash value will be modified.

This ledger consists of individual blocks which store data in a specific format. The necessary data generally stored in Blockchain is:

- Data
- Previous Hash
- Time Stamp

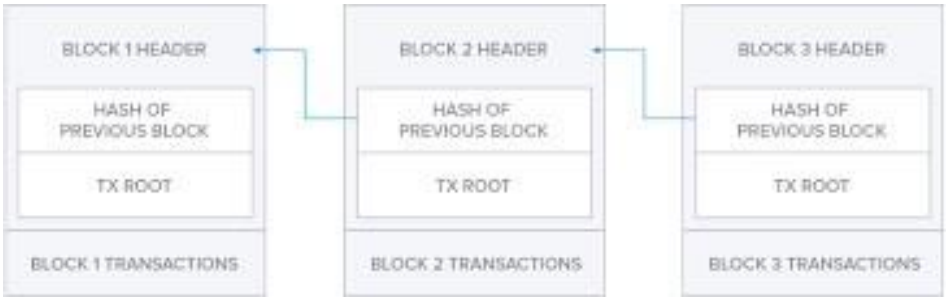

Figure 1: Representation of Blockchain

3.2 Ethereum

Ethereum is a Blockchain based open source software network and an operating framework incorporating smart contracts. Ether is the crypto-currency created on the blockchain of Ethereum and can be exchanged between different accounts. It also offers a shared virtual machine from Ethereum that can run the scripts using a distributed public node network. Ethereum offers a platform for development of decentralised application based on the smart contract.

3.3 Smart Contract

A smart contract is a code running on top of a blockchain that includes a series of rules by which the parties to the smart contract decide to communicate under certain circumstances with each other. When the particular event happens the code in the contract should be implemented.

3.4 Decentralised Application (DApps)

Decentralised applications are applications not having a centralised infrastructure. This utilizes shared storage and connectivity, meaning that most DApps have their backend application running on a public peer-to-peer network, in this case, a blockchain, while A typical software arrives with its backend technology running on centralised servers.

DApp = Frontend + Blockchain based Smart-Contracts

4. Implementation

The entire application was developed, keeping in mind the various requirements of an organisation and the educational institutions which are storing the data on the portal.

There are two layers of abstraction in the application:

i. The general user can just see the final percentage and specific details like department, graduation year, final CGPA and Percentage.

ii. A verified employer/ University/Organisation can have a look at marks in all subjects throughout the course of the University. To get verified, the organisation would need to authenticate themselves using their official email id.

The Software Stack includes the following:

1. A Blockchain-based Smart Contract written in Solidity.
2. An Interactive ReactJS based web application written in JavaScript.
3. A Python-based parser for parsing a large amount of data containing student credentials and storing it into the Blockchain, which interacts with a shell script for storing the data into the Blockchain.

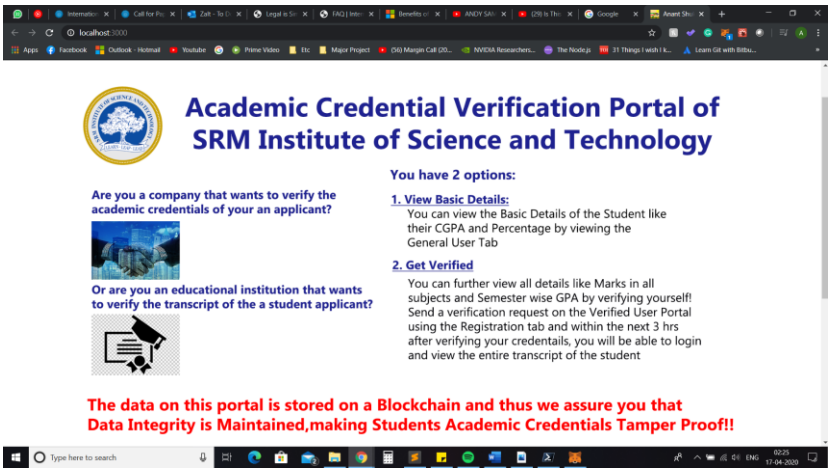

Figure 2: Homepage of Academic Verification Portal

4.1. The Blockchain Based Smart Contract

The Blockchain is written in Solidity, which is a language based on JavaScript, which is used to write Smart Contracts in Ethereum. The smart contract includes the following modules:

1. **Create Student:** This module creates the student ID into the Blockchain. This module is only available to the Admin.
2. **Enter Student Details:** This module is responsible for entering the student credentials and marks of the students into the smart contract. This module is only available to the Admin.
3. **Get Students:** This module returns the student ID of all the students in the Blockchain. This module is viable only to the Admin.
4. **Get Student Details:** This module returns the credentials of the student that has been taken as input.
5. **Get Student marks**: This module returns the marks of the student that has been taken as input. This module is only accessible by the Verified Users and the Admin
6. **Count Students:** This module maintains the total number of student credentials in the smart contract

After the smart contract was written, test scripts were written in JavaScript and tests were conducted on all the modules of the smart contract with the help of Truffle. Truffle uses the Mocha testing framework and Chai for assertions to provide a framework to write the JavaScript tests.

After receiving the data from the test files, the modules were further optimised to make sure that the Gas Requirements were minimal, and modules were functioning correctly and efficiently. This would help us in making sure that our application works seamlessly and flawlessly.

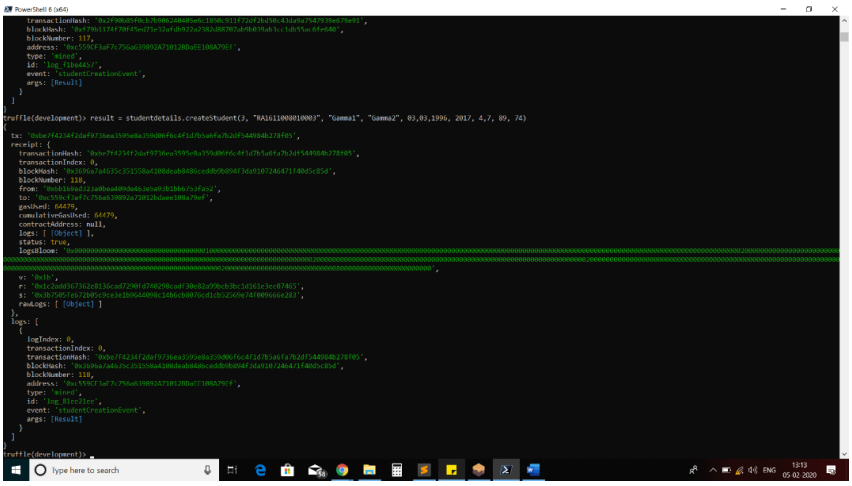

Figure 3: Smart Contract Testing

4.2. Web Application

The Web Application is an application based on React, which is a JavaScript library for building user interfaces. This Web Application interacts with the Blockchain with the help of the Web3, which are a collection of libraries which allow us to communicate with an Ethereum node, using an HTTP or IPC connection.

We use MetaMask, which is an extension, enabling us to access Ethereum enabled distributed applications from our browser. Metamask injects the Ethereum web3 API into a website's JavaScript context. Therefore, the Distributed App can read from the Blockchain.

The Web Portal is an entirely secure portal in which data can be inserted and retrieved with the Blockchain. The Web Portal is divided into various modules. These have multiple roles; some have been used for support to the Admin, and others are for the end-user. They all bind together to make a seamless and interactive app.

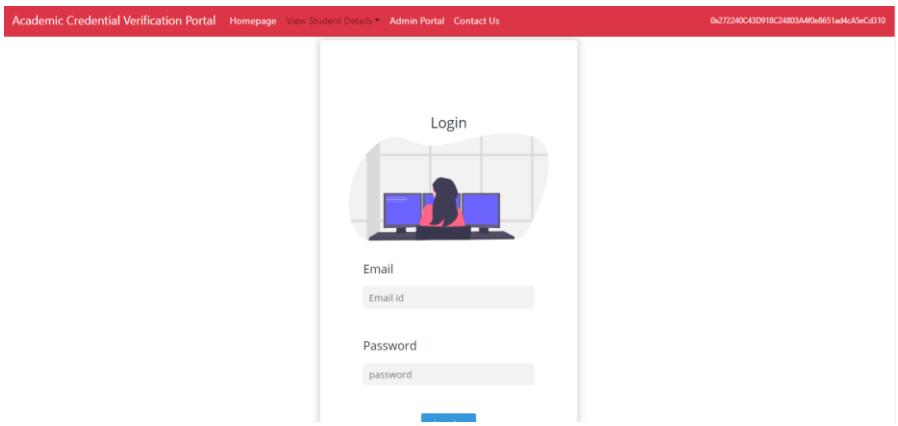

Figure 4: Admin Portal of our Academic Credential Verification Website

Some of the significant modules are mentioned below:

1. **Admin Portal:** This is the Administration Portal where the access is given to the Admin for making student Entries and verifying data from time to time. The admin portal also grants verification status to the users who want

to see a complete transcript of the student with all student marks and semester GPA.

2. **General User Portal:** The General User will have access to just necessary details like the overall CGPA and Percentage and Date of Birth. If the organisation wants to view further information, they can register themselves for verification status on the Register tab in the portal.
3. **Verified User Portal:** The Verified User Portal is the lowest level of abstraction in the application for the end-user. An authenticated user can have a look at all student details like their marks in each subject and GPA in each semester.

4.3. Parser

The first stage of the parser is written in Python, which reads the data from the records and stores it into a batch file in the required function format. The second stage is a shell script which reads the data from the batch file and enters it into the Blockchain by accessing its shell. After entering the data, the data is verified with the original records to check for any discrepancy. After the verification is complete, the information is pushed into the Blockchain.

5. Results

The problem of manual authentication of each certificate can be solved by saving the Blockchain encrypted certificates. The Blockchain platform makes transactions unchangeable and openly verifiable; these Blockchain properties are used to produce digital certificates that are flawless and simple to check.

We have developed a web portal which is linked to the Blockchain that stores the academic credentials of all the students who have graduated from the University. The potential employer/ educational institute can access a web portal designed by us to verify all details of the students after providing necessary credentials given to them by the student (example: a combination of Registration number and Date of Birth).

With the help of our applications. The digital certificates are stored on an Ethereum Blockchain. Our solution is scalable, and because of the use of Blockchain, it provides immutability.

As the backend is handled by the Ethereum Network, we do not have to worry about the overhead costs. This makes maintenance costs cheaper significantly. We have tabulated the cost of some operations, which helped us to come to the conclusion that the Ethereum Blockchain is highly cost-effective in comparison to other Blockchain Systems:

	Activity	**Cost in ETH**
1.	Deployment of Smart contract on the Ethereum Network	0.012551
2.	Cost for addition of a single student credential	0.0000458
3.	Cost for addition of 10 student credentials	0.0003206
4.	Cost for addition of 50 student credentials	0.001603
5.	Cost for addition of 100 student credentials	0.003024
6.	Cost for addition of 1000 student credentials	0.02406
7.	Cost for Retrieval of Data	0

Table 1: Cost for Transactions on the contract

We also analysed the block size and Transaction time for insertion of Student Details in the Blockchain for all the student details. Here we came to the conclusion that the Ethereum Blockchain is highly Size optimized.

	Block Size	**Block Size (Average)**	**Processing Time**	**Gas Limit**	**Gas Used Per Transaction (Average)**
1.	**Block Size of 1 Student**	186 bytes	3.2 seconds	77985	51990
2.	**Block Size of 10 Students batch**	186 bytes	34 seconds	77985	52610
3.	**Block Size of 50 Students batch**	186 bytes	168 seconds	77985	51460
4.	**Block Size of 100 Students batch**	186 bytes	342 seconds	77985	52110
5.	**Block Size of 1000 Students batch**	186 bytes	3560 seconds	77985	52240

Table 2: Comparison of Block size and Processing time

Our survey of the existing solutions and found our solution to be one of the best solutions that was highly extensible. Below is a table comparing the various solutions currently available.

Scheme	System Features			Security Features				Usability		
	Accreditation	Verification	Revocation	Counterfeit Protection	Privacy	Selective Disclosure	Transparency	User Experience	Key No Management	Accessibility
UNIC	-	❍	-	❍	●	-	●	●	●	●
Blockcerts	-	●	❍	❍	●	-	●	●	-	●
Hypercert	-	●	❍	❍	●	-	●	●	-	●
Echo	-	❍	-	❍	-	-	●	❍	-	❍
UZHBC	-	❍	-	❍	●	-	●	●	●	●
EduCtx	●	❍	-	●	●	-	❍	❍	-	❍
Blockchain for Education	●	●	❍	●	●	-	●	●	●	●
Cerberus	-	●	●	●	●	-	●	●	●	●
Our Academic Verification System on Blockchain	●	●	-	●	●	●	●	●	●	●

❍= provides property; ● = partially provides property; - = does not provide property

Table 3: Summary comparison of various solutions

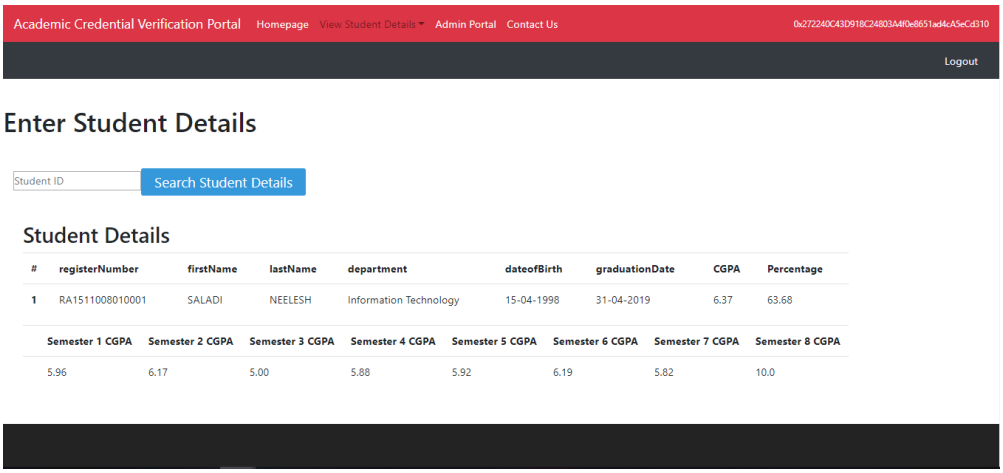

Figure 5: Verified User Portal on our Website

Credential theft is an aggressive phenomenon in educational institutions that threatens corruption and involves high economic costs. People often hack or fraud with their documents. Unfortunately, the earlier techniques of credential validation were time-consuming, expensive and involved many people. In this paper, we have presented a robust blockchain-based approach which counters instances of fraud, as well as provide significant improvements within terms of usability, performance and comfort over traditional systems. Blockchain provides a platform or forum to hold a secure and verifiable record of academic credentials. This platform ensures that ones' identities are checked indefinitely, transparently and are cryptographically protected, and thus the confidentiality is secure. This project is planned with the demands of fields of education and recruitment that will be beneficial for both the organisation and the students. Entities such as recruiters, employees, the

government can validate student credentials in just minutes without depending on a central authority.
The University can promise the authenticity of this data as this is stored on a blockchain and any modification of data can be easily detected and prevented from propagating to the rest of the Blockchain.

6. Discussion

Benefits:

- No third-party involvement: This methodology would prevent the participation of the third party in the process of validation of academic credentials.
- The portal is accessible 24 / 7: Since this will be an online portal, it will be readily available to the authorised users whenever and wherever required.
- Robust data security: Since the system uses blockchain technology, it ensures high transparency, offering a more secure network to store students' private data. Any change made to the data is easily traceable, thus minimising risk to forgery of data.
- Environmentally Safe: Since the whole system will be digitalised, it will help in saving paper and time, thus contributing to environmental sustainability.

Difference between the current and the existing system:

- Workflow enhancement: The system will ensure that the academic qualifications of any employee or employee applicant can be easily verified and is accessible immediately to the user, thus providing more efficiency.
- Transparency of the system: The site will be publicly accessible. Use of Blockchain would ensure that no-one can hack or cipher the data.
- Reduced time and cost limitations: By having the ability to check and view an individual's academic credentials instantly, employees and users will now reduce the cost and time delays associated with the current authentication process.
- Comprehensive data accessible to approved/authorised users only: Only an authorised user can access to detailed student data. This will allow student data to be confidential.
- Putting back the trust in education: When institutions merge with other bodies or there is war or other natural calamities, the academic data will be safe and protected.
- No more fake certificates: There will be no more morphed certificates as certificates will be digitally verified.
- Multiple verifications at once: Multiple certificates are verified once at the time.

ISSN: 2005-4238 IJAST

Appendix

The code has been completed and the same is available as a web application on Heroku. The link to the application is:

https://academic-credential.herokuapp.com

or

https://anantshukla.github.io/academic-credential-verification

The following are the pre-requisites for running the application:

- You need to be connected to the Ethereum network. There are many extensions available to connect to the Ethereum Network. One such application is MetaMask. It can be installed on Google Chrome or an.
- You need to be connected to the Kovan Test Network. Test networks in Ethereum are Networks where you can test your smart contracts and their functionalities. You can connect to the Kovan Test Network by choosing the same in MetaMask.
- JavaScript should be enabled in your Browser.

References

[1] Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," www.bitcoin.org.
[2] Hailong Yao, Caifen Wang, "A Novel Blockchain-Based /Authentication Key Exchange Protocol and Its Applications," 2018 IEEE Third International Conference on Data Science in Cyberspace.
[3] Marco Baldi, Franco Chiaraluce, Emanuele Frontoni, Guiseppe Gottardi, "Certificate Validation through Public Ledgers and Blockchains," In Proceedings of the First Italian Conference on Cybersecurity (ITASEC17), Venice, Italy.
[4] Haveman, Robert, and Timothy Smeeding. "The role of higher education in social mobility." The Future of children (2006): 125-150.
[5] Hanushek, Eric A., and Ludger Woessmann. "Education and economic growth." Economics of education (2010): 60-67.
[6] Hanushek, Eric A., and Dennis D. Kimko. "Schooling, labor-force quality, and the growth of nations." American economic review 90, no. 5 (2000): 1184-1208.
[7] Coulombe, Serge, Jean-François Tremblay, and Sylvie Marchand. Literacy scores, human capital and growth across fourteen OECD countries. Ottawa: Statistics Canada, 2004.
[8] Schweinhart, L., and Z. Xiang. "Evidence that the HighScope Perry Preschool program prevents adult crime." In American Society of Criminology Conference. 2003.
[9] Reimers, Fernando. "Citizenship, identity and education: Examining the public purposes of schools in an age of globalization." Prospects 36, no. 3 (2006): 275-294.
[10] Transparency International. Global corruption report: Education. Taylor & Francis, 2013. Available: https://www.transparency.org/whatwedo/publication/global_corruption_report_education.
[11] T. Bui, T. Aura, "Key Exchange with the Help of a Public Ledger," F. Stajano, J. Anderson, B. Christianson, V. Matyáš (eds) Security Protocols XXV.
[12] Security Protocols 2017. Lecture Notes in Computer Science, vol 10476. Springer (2017).
[13] Grolleau, Gilles, Tarik Lakhal, and Naoufel Mzoughi. "An introduction to the economics of fake degrees." Journal of Economic Issues 42, no. 3 (2008): 673-693.

[14] "Education: Sending Degrees to the Dogs", TIME.com, 2019. [Online]. Available: http://content.time.com/time/magazine/article/0,9171 ,954229- 1,00.html.
[15] Sansiti, M. and R. Lakhani, K. (2017). The Truth About Blockchain. [online] Harvard Business Review. Available at: https://hbr.org/2017/01/thetruth-about-blockchain.