

A Synopsis on

# Online certificate Generation & Authentication using Blockchain

Submitted in partial fulfillment of the requirements

of the degree of

Bachelor of Engineering

in

Information Technology

by

Prasad Jadhav (17104003)

Aseem Godambe (17104058)

Rutwik Gaikwad (17104074)

Prof. Kiran B. Deshpande

Prof. Kaushiki Upadhyaya



Department of Information Technology A.P. Shah Institute of Technology  
G.B.Road,Kasarvadavli, Thane(W), Mumbai-400615 UNIVERSITY OF  
MUMBAI 2020-202

## CERTIFICATE

This is to certify that the project Synopsis entitled 'Online certificate Generation & Authentication using Blockchain" submitted by Prasad Jadhav (17104003)", Aseem Godambe (17104058)", Rutwik Gaikwad (17104074)" for the partial fulfillment of the requirement for award of a degree Bachelor of Engineering in Information Technology to the University of Mumbai, is a bona fide work carried out during academic year 2019-2020

(Prof. Kiran B. Deshpande)

Guide

Prof. Kiran Deshpande

Head Department of Information  
Technology

Dr. Uttam D.Kolekar

Principal

External Examiner(s)

1.

2.

Place: A.P. Shah Institute of Technology, Thane

Date

## Declaration

We declare that this written submission represents my ideas in my words and where others' ideas or words have been included we have adequately cited and referenced the original sources. We also declare that we have adhered to all principles of academic honesty and integrity and have not misrepresented or fabricated or false ed any idea/data/fact/source in our submission. We understand that any violation of the above will be cause for disciplinary action by the Institute and can also evoke penal action from the sources which have thus not been properly cited or from whom proper permission has not been taken when needed.

(Signature)

(Prasad Jadhav - 17104003)

(Aseem Godambe - 17104058)

(Rutwik Gaikwad - 17104074)

Date:

# Abstract

In the modern digital age, the advancement in technology has resulted in solving complex problems. But this advancement has also resulted in increased illegal activities. One such major activity is forgery of documents and certificates of an individual. When applying for a job interview or further studies there is no way to verify the certificates or degree submitted by an individual is genuine and not a forged document. The only way is to contact the respective administration to verify the same. But this method is very time consuming and costly. To resolve this issue, we make use of blockchain technology. This digitalizes the certificates and verifies the originality of the certificate. Using this method, a person can verify if the provided certificate or degree is forged or not.

In this research Ethereum Blockchain is used to create the blockchain as its open source platform. Since this is an open source platform, the project becomes very cost effective and also easy to execute. In this project the verification can be done through the unique hash value given to each and every certificate, which makes the certificate unique and hence it cannot be used by anyone else as a duplicate certificate.

This research would focus on providing a secure and simple way to distribute certificates to its rightful owner and hence will avoid any duplication. Due to its efficiency in cost and workload it can be deployed in any big institute or a university as well, to solve the major issue that most of the institutes face.

# Introduction

In today's world, there is a huge competition for jobs. The companies need skilled employees for their jobs. Certification is a great way to prove your expertise in any field of work. People from various backgrounds can learn a skill online and apply for the exam and get certified. But with the advancement in technology some people try to cheat the system by creating fake certificates and degrees. This forgery further leads to unskilled individuals which are the future of the society. To cater to this problem a system was needed which could verify that the degree and the certificates represented by an individual are genuine and not a copy. So basically, a system which could validate the certificates received by an individual from respective authority with ease. This is where blockchain comes into the picture. Blockchain features a decentralized and incorruptible database that has high potential for a diverse range of uses. Blockchain is one of the wide spreading technologies. It has a distinct feature and use in verification of the documents.

Blockchain can be designed as a public ledger which is used to store all the transactions in the system in a decentralized manner. The key features of blockchain are that it cannot be tampered, the transactions are traceable and it provides security with the help of encryption. For this system we have decided to use Ethereum Blockchain which is an open source platform. The system also ensures to cater the common issues faced by an educational institute.

# Objectives

The main objective of this project is to create a simple and secure application with various features which can be used in colleges and big institutions. The nished application will have the features as follows:

- This system should have a secure and simplified way for distribution and verification of certificates which only the admins can handle. The system should enable the admins to issue certificates which can be either selected from a template or a customized certificate design can be uploaded.
- It should have a simplified way to upload multiple certificate data for the certificate issuer. The issuer will have to just upload the CSV le of all the certificate data which needs to be printed on the certificate. After uploading, the data should automatically fill the missing space on the certificate to complete the certificate of the individual.
- It should have ease of access to all the certificates issued and verification possible at the click of a button. A mail should be sent to the certificate holder with a link to the certificate. The system should allow resharing and verification by anyone who has the link for the certificate.
- The application should have an e ective veri cation and validation system to ensure the genuinity of the certificate. The data should be directly fetched from the blockchain network and generation of certificates should take place to ensure there is no tampering of the data.

# Literature Review

The first idea of collecting various certificates and documents in one block was led out by [1]Stuart Haber and W. Scott Stornetta back in 1991. Their basic idea was to create a system in which the documents and certificates cannot be tampered by anyone. They decided to implement it using a cryptographically secured chain of blocks. This further led to the concept of blockchain which was introduced in 2008 by Satoshi Nakamoto (or group of people). At the initial stage blockchain was focused on crypto-currency. But later on, blockchain extended in various other fields. Blockchain could also be considered as an online ledger which can provide decentralized and transparency in data sharing.

The concept of blockchain was to store data in a block along with a timestamp. Once the data is entered into the block and it is verified then it becomes immutable and open in public to provide transparency. The block is provided with a hash value of the current block and also the hash value of the previous block in the chain. This ensures the trackability of the block from the chain.

The advancement in the field introduced Ethereum into blockchain. Ethereum focused on other usage of blockchain. This led to the division as Bitcoin was for payment network Ethereum started its use in computing. The other advantage of Ethereum was that it was an open source project.

Ethereum introduced EVM i.e. Ethereum Virtual Machine. These are programmable blockchain. It works on a high-level language developed for this purpose like Solidity. It also has a smart contract. [2]Smart contracts basically streamlines multiple complex tasks or processes involved in completing an objective. Smart Contracts basically work on a simple statement 'if/when. . . then. . .'. It's just the coding done to perform tasks automatically if one situation occurs then what would be its countermeasure. Smart contracts not only have the same time but also provide reliable security. The various aspects of smart contracts are self-verifying and self-executing. It is also tampering resistant, involves less intermediaries and also has low transaction cost.

The papers referred to while developing the system are mentioned below:

1. [3] Online Certificate Validation Using Blockchain. - Special Issue Published in Int. Jnl. Of Advanced Networking Applications (IJANA)

Author: Shanmuga Priya R, Swetha N - Department of Computer Science and Engineering, Prathyusha Engineering College, Thiruvallur, TamilNadu

This document summarizes the problems of forged certificates and how blockchain can solve the issue. Netbeans IDE and Android Studio are used to develop the server communication and the application to scan the QR codes. EthereumJS is used for faster Ethereum applications. The application involves the user uploading his/her certificate like 10th-grade mark sheet, college certificates, government certificates, and so on to the portal. After uploading the certificate, the data is then sent to the issuer for validation. The issuer (eg. School for validation of 10th Marksheet) has to validate the data received by the application for verification. Once verification is successful, the data will be stored on the server else it would be discarded. On the mobile application, a QR code will be generated based on the certificate number. The QR code can then

be shared with anyone else for verification in case of necessity. When the QR code is scanned, an OTP will be sent to the registered mobile number for verification. After proper authentication, the user can view the certificate. If the number of scans goes beyond the permitted limit, the location of the scanner will be sent to the authorized user with a permission link. From that link, the authorized user can either allow or deny the person.

The major drawback of this system is that verification can be delayed by the issuer as the certificate has to reach the organization for verification and the data is sent to blockchain only after verification. The OTP system can get tedious. This system can get costly as well.

[4] Certificate Verification System using Blockchain International Journal for Research in Applied Science Engineering Technology (IJRASET)

Author: Nitin Kumavat, Swapnil Mengade, Dishant Desai, JesalVarolia.

This document summarizes that during the course of education the students achieve many certificates. Students produce these certificates while applying for jobs in public or private sectors, where all these certificates are needed to be verified manually. There can be incidents where students may produce fake certificates and it is difficult to identify them.

The solution proposed in this system uses Ethereum and IPFS (Inter planetary le system). IPFS is a peer to peer, content address system. It is very similar to BitTorrent and MerkleDag. Unlike HTTP which restricts or provides low latency on transfer of large amounts over the network which uses IP addressing, IPFS uses content addressing. As a result it creates a distributed system of different nodes across the network. It returns us a hash value and it uses this value to retrieve the data.

They propose to add the data with the certificate on the IPFS network to generate the hash for it and later on add the data to the blockchain network with the help of EVM. This topology includes two distributed networks to provide additional security to the model. While retrieving the certificate they would compare the hash and pull the entire certificate which has been stored on the IPFS network.

The advantage of this system is it is more secure, provides reliability. With two distributed networks, it's almost impossible to tamper the data.

On the other hand, the disadvantage of the system is that IPFS is a tedious process to set-up as well as storing the certificate image on any distributed blockchain platform costs a lot of money and hinders the scalability of the system.



## Problem Definition

Currently, the certificates are stored in a centralized manner and verified manually, so it takes too much time to verify. There is no safety to the certificates that are given to any private sector (banks). But the data may be changed, deleted, or modified.

Certificates are easily hacked and it is easy to make a duplicate of that certificate. Students bring their certificates to interviews. It also takes a lot of time to get the certificates verified and it is also difficult to maintain the record manually.

## Proposed System Architecture/Working

The proposed architecture uses blockchain technology to provide a solution. As blockchain provides a secure and distributed network to store the information it becomes an optimal solution. Ethereum is a type of cryptocurrency used for this research. It stores the data in both text as well as image format but the cost to store in pictorial format is way higher than in text format as Ethereum gas is consumed which depends on the size of data which is being uploaded on the network. The prices vary daily on the basis of the transaction happening in the network.

It may be noted from the solutions that the cost of storing one certificate is very high and it would be practically impossible for small organizations to opt for this method to store a huge number of certificates. It has been observed that many organizations have a similar look for their certificates. In different competitions conducted, certificates are given to winners and runner-ups. These certificates have a similar pattern, rather similar design, and only the parameters, like name, etc in the certificate change from one certificate bearer to another. To solve this issue we have proposed a different method to store the certificates.

The system involves storing the certificate data in two parts. The first part includes storing the template of the certificate which will be uploaded by the admin in SVG format. This template will have text fields for all the variable parameters. These text fields will be given ID relevant to the information that will be displayed on the template. The template uploaded by the admin will be stored on the file system. To provide enhanced security, the templates can be stored on the InterPlanetary File System so that the SVG template will also be stored on the blockchain.

The variable data, e.g. name, certificate ID, place secured, etc will be uploaded in a CSV file to the website. This CSV data will be validated, mapped and a preview is provided for the user to verify if the certificate template maps the data correctly to the respective fields for the correctness of the certificate. Once the data is uploaded after validation, each row is converted into a short JSON which also includes the hash and the ID of the SVG. This JSON object is then stored on the Ethereum Blockchain via the Smart Contract.

When the user tries to fetch a certificate from the website using the Certificate ID or the URL, a request is made to the Ethereum Blockchain with the corresponding Transaction Hash to fetch data. If any JSON object is found, the data from the BlockChain is fetched and formatted. From the server, the SVG with the corresponding certificate ID is fetched and displayed. The text fields of the SVG are then populated with the data received from the JSON object and displayed to the user. The user can also manually verify the records on the BlockChain. The Etherscan portal allows anyone to view the raw transactions done to the blockchain. When the transaction hash is provided, the raw JSON object can be seen directly on the blockchain. This provides transparency and security to the system.

- Module 1: Certificate Generation and Verification

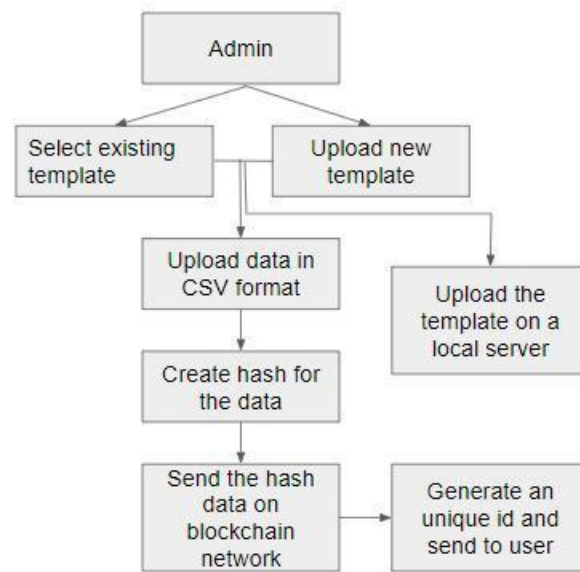


Figure 1: Block Diagram of Admin-side System

This module demonstrates the working of the admin side of any organisation willing to use the platform to generate digitized secure certificates. First step the admin should upload the certificate template in the SVG format or choose from the existing templates previously uploaded by the admin for his organisation. The SVG format is mentioned so that later on the certificates could be generated dynamically. In the second step the admin could upload the data of the users to whom the certificates are needed to be awarded. The CSV document would also contain all the other necessary fields on the certificate like the issuing or expiration date of the certificate. Once the data is uploaded by the admin the certificate template would be indexed and would be stored on the non distributed server so as to save the cost of uploading an image on a blockchain network. The data of the respective certificates would be hashed along with the index of the certificate and would be stored on a distributed network with the help of EVM. When the data is uploaded on the network the user to whom the certificate has been issued would receive a URL for the particular certificate. In this way the data is stored on the secure distributed blockchain network. It also prevents the uploadation of expensive images of the certificate on the blockchain network which cost multiple times when compared to normal text based format.

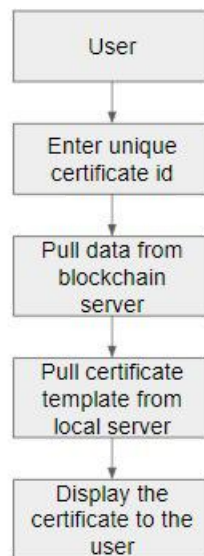


Figure 2: Block Diagram of Proposed User-end system

On the users end an individual could verify the certificate by just entering the url of the certificate on the portal. If the url is right the appropriate data would be fetched from the blockchain network. This data would be decoded and the certificate index would be extracted from it. Using this index number an appropriate certificate would be pulled from the non distributed server. Once the certificate template and data is retrieved the data would be mapped on the right elds of the certificate like the name of the individual, expiration date of the certificate and other di erent elds.

So just by pasting the URL of the certificate we could verify the authenticity of the certificate holder.

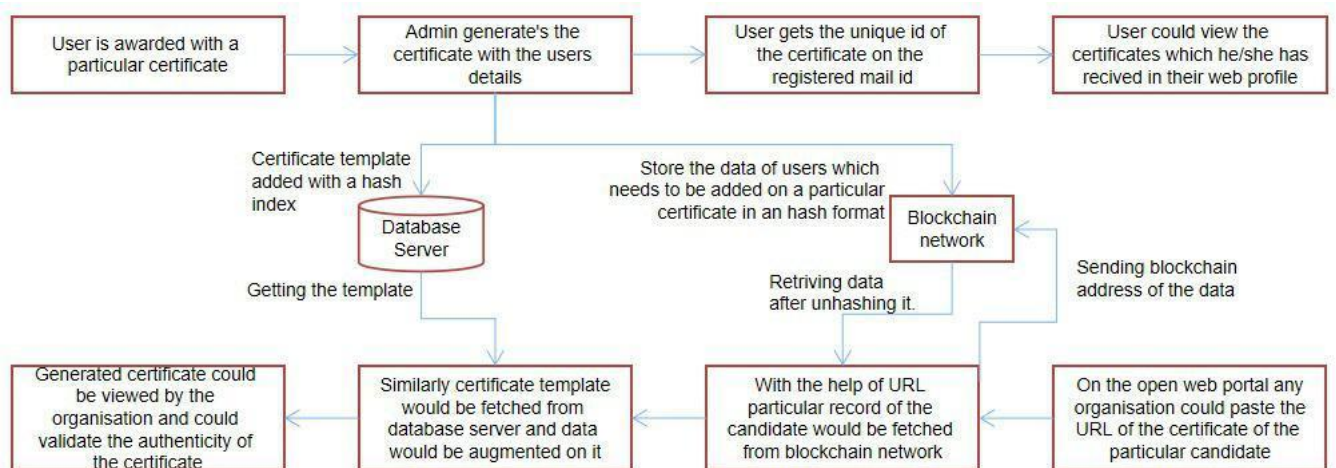


Figure 3: Full architecture of the proposed system

## Design and Implementation

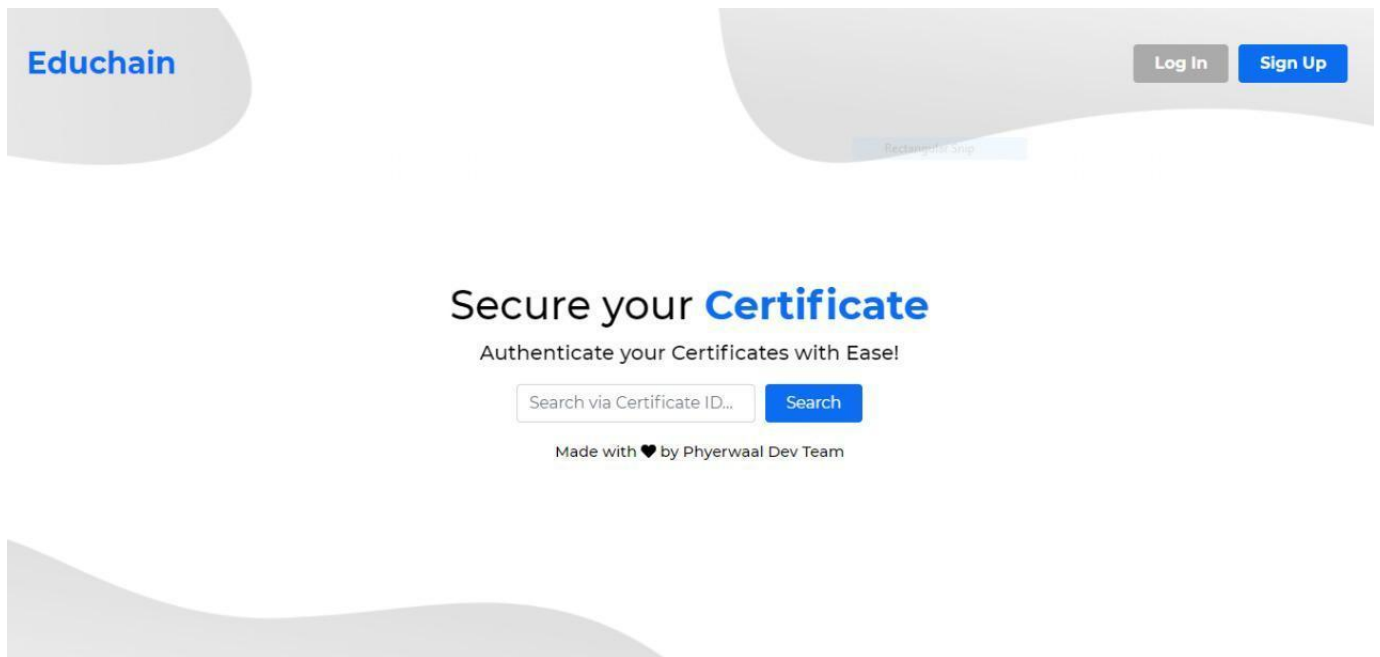


Figure 4: Home page

The above screen is the home page of our application. This is the landing page that the user sees after he visits the URL. A certificate can be searched by anyone from the search box provided. The user can search for a certificate by the certificate ID or the Transaction Hash provided to the user. The Login and Sign up buttons allow the user to login to see all his/her certificates.

## Login

Email address

We'll never share your email with anyone else.

Password

☐ Login as Admin (Toggle if Admin)

[Forgot Password?](#)

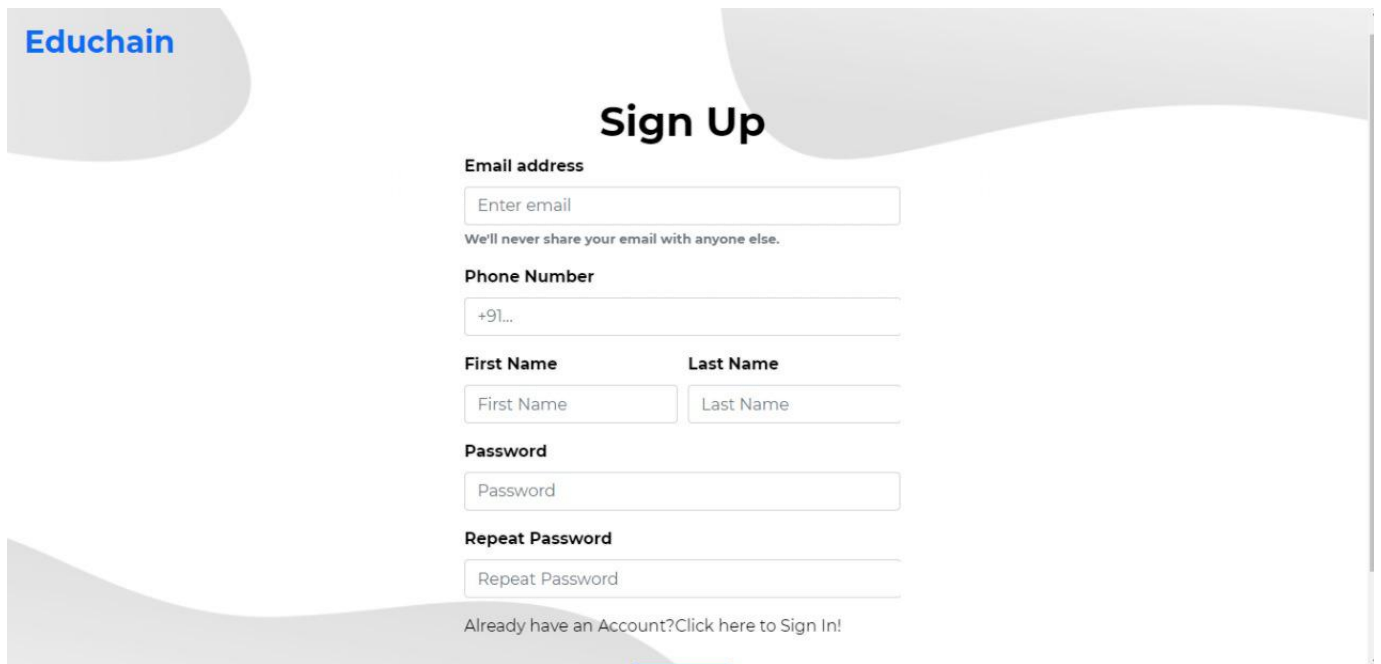
[Don't have an account? Click here to create one!](#)

Submit

Made with ❤ by Phyerwaal Dev Team

Figure 5: Login portal

The user can log in to the portal to view all his certificates that have been issued for the registered email ID. The password provided is hashed for security purposes. The toggle can be used to login as Admin. The admins can log in to add new certificate data.



**Educhain**

## Sign Up

**Email address**

We'll never share your email with anyone else.

**Phone Number**

**First Name** **Last Name**

**Password**

**Repeat Password**

Already have an Account? [Click here to Sign In!](#)

Figure 6: Sign-up portal

The sign up page can be used by the user to create a new account for viewing all his/her certificates. When a new account is created, a verification mail is sent to the user's Email ID for verification. Once verified, the user can log in to view his/her certificates

Figure 7: Template uploading portal

When an admin logs in to the portal, he can add a new template of certificate or select an existing template to allow reusing of certificates to occupy less space and reduce cost. The template should be uploaded in an SVG format, the details of which have been provided in the documentation for easy creation of the template.

Figure 8: Admin Dashboard

On this page, the admin can upload the data in a CSV file to be stored on Blockchain. The headers of the CSV file map to the data fields of the SVG template to provide a preview of the final certificate. In case of any errors, the admin can reupload the CSV before submitting it to the blockchain. The admin must verify using the preview option to check if all the data is correctly mapped to the certificate and that it has a proper orientation.



Verified 

ISSUER

APSIT

TXN ID

0xc33d3514a369b2c57f1ec29354855da376d2019a39615d7  
7c4955d8a8ec2c

Figure 9: Validated certificate

Once a certificate has been issued to a candidate, an Email is sent to the candidate with a verification link to check the certificate. The certificate's template is picked up and the data is fetched from the blockchain. After successful fetching, the data is mapped to the template and a proper certificate is printed on the screen. The transaction hash is also printed for verification.

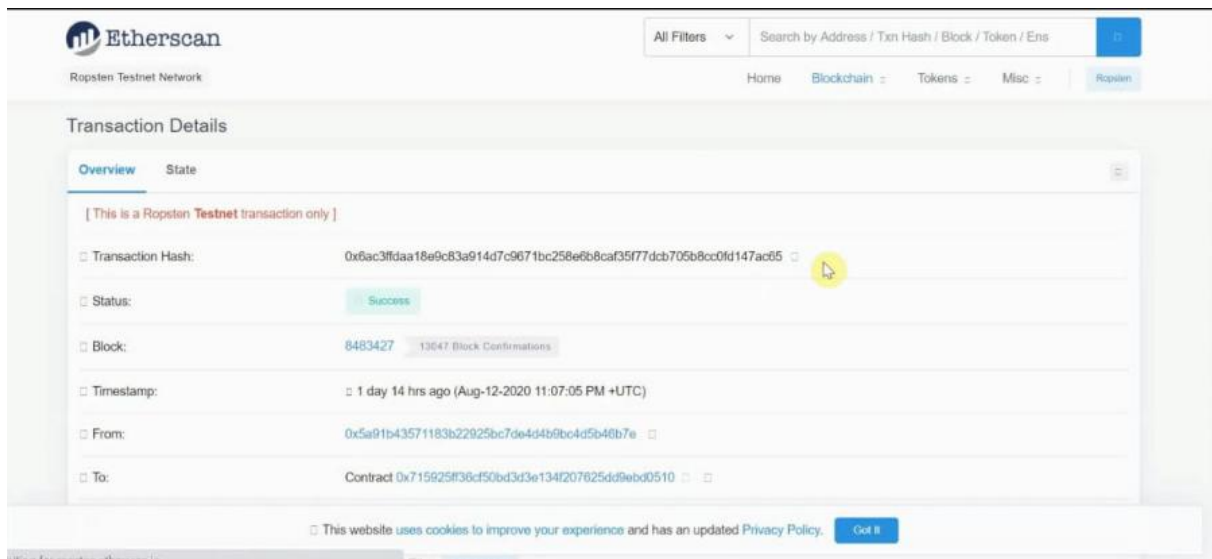


Figure 10: Record of block creation

On clicking the transaction hash on the verification page, the transaction can be viewed on the Etherscan website with proper authentication details. The data of the certificate along with the certificate name and slug can be seen in the Input Data eld. The input data can be changed to UTF-8 to read the contents as it is visible in binary format.

## Summary

In the current scenario certificate validation is difficult and usually, time-consuming. To cater to this problem, this application can be used to verify that the degree and the certificates represented by an individual are genuine and not a fake copy. This system uses blockchain technology as its core in its technical stack. Blockchain features a decentralized and incorruptible database that has a high potential for a diverse range of uses. It has a distinct feature that can be used for verification of the documents. This project uses Ethereum Blockchain to create its network as it is an open-source platform. This makes it cost-effective and easy to implement. In the blockchain, the verification can be done through the unique hash value given to each and every certificate, which makes the certificate unique, and hence it cannot be used by anyone else as a duplicate certificate. This application has a single secure portal for users and the administrators or certificate issuers. But first, the users and the administrators must be registered to the system to use all the utilities of the system i.e. to create and retrieve the certificate with ease. The issuer can upload certificate templates and their data and it would be passed on to the system. Later on, the certificate would be given only to its rightful owner, with each certificate having a unique hash value. With this implemented it can be said that this application will provide a secure and simple way to distribute certificates to its rightful owner and hence will avoid any duplication, without raising a hefty cost to the institutions and also deploying it with ease.

## References

[1] Blockchain:

<https://en.wikipedia.org/wiki/Blockchain>.

[2] Smart Contracts:

<https://www.ibm.com/blogs/blockchain/2018/07/what-are-smart-contracts-on-blockchain/:text=Smart>.

[3] Shanmuga Priya R, Swetha N. Online Certificate Validation Using Blockchain. Published in Int. Jnl. Of Advanced Networking Applications (IJANA) <https://www.ijana.in/papers/37.pdf>

[4] Nitin Kumavat, Swapnil Mengade, Dishant Desai, JesalVarolia (2019). Certificate Verification System using Blockchain. International Journal for Research in Applied Science Engineering Technology (IJRASET). <http://ijraset.com/leserve.php?FID=20914>

[5] What Is Blockchain and why should records management professionals care?, <https://www.ironmountain.com/resources/general-articles/w/what-is-blockchain-and-why-should-records-management-professionals-care>

[6] Oliver Miquel, Moreno Joan, Prieto Gerson, Ben tez David (2018). Using blockchain as a tool for tracking and verification of official degrees: business model 29th European Regional Conference of the International Telecommunications Society (ITS): "Towards a Digital Future: Turning Technology into Markets?", Trento, Italy, 1st - 4th August 2018 <https://www.econstor.eu/bitstream/10419/184958/1/Oliver-et-al.pdf>

[7] Blockcerts:

<https://www.blockcerts.org/>

[8] Document verification system using blockchain:  
<https://www.blockchain-council.org/blockchain/document-verification-system-using-blockchain/>

[9] MetaMask:

<https://www.sitepoint.com/metamask-ethereum-blockchain/>

[10] Ganache:

<https://www.trufflesuite.com/ganache>

[11] Ethereum:

<https://www.tutorialspoint.com/ethereum/ethereum-ganache-for-blockchain.html>

## Plan of Paper Publication

- We have decided to present a paper in IEEE 2021 International Conference on Computing, Communication, and Intelligent Systems (ICCCIS).
- We are ready with the abstract, introduction as well as literature survey.
- The advancement in our project is that the certificate templates would be stored on the local server rather than adding it to the blockchain network; this would save a lot of money.

