VEER SURENDRA SAI UNIVERSITY OF TECHNOLOGY, ODISHA, BURLA

सिद्धिर्भवति कर्मजा

DECENTRALIZED CERTIFICATE VALIDATION SYSTEM USING ETHEREUM BLOCKCHAIN

Guided by:

Mrs. Santi Kumari Behera

Submitted by:

Ajay Kumar Pradhan

Alok Kumar Patro

Department of Computer Science and Engineering

VSSUT Burla, Odisha

Contents:

1. Introduction
2. Literature Survey
3. Background Study
   - ❖ What is Blockchain Technology?
   - ❖ What are Smart Contracts ?
   - ❖ What are Distributed Ledgers?
4. Work Done
5. Results
6. Conclusion
7. Future Scope
8. References

Introduction

With internet being a necessary part of modern human life, unethical practices have also come to a rise. Our countermeasures to such unethical practices however haven't evolved as fast.
Fake certificates, loans, online frauds, fake products etc have become rampant and it has become hard to deal with them as the vast and easy availability of internet has boosted such acts to a level that one can't easily differentiate to what is authentic and what is fake.

This results in lack of trust and monetary loss for both parties while a unethical middle man gets benefits.

Certificates in educational institutions have been issued in the same way for decades now. Even after digitization of the records, the basic structure has remained same; this leads to producing fake and doctored certificates from individuals to take undue advantage of the degree.

Introduction

This greatly hampers the hiring process for students where the companies have to employ background check services which verify the authenticity of the certificates almost entirely manually which aren’t foolproof either. This results in delay in hiring process, which hampers both the companies and the students.

This project gives an walkthrough as to how a cost effective and efficient solution to this problem can be reached by using Blockchain.

Literature Survey

[1]. Certification.io:

Certifaction.io provides a blockchain platform where they save encrypted documents to their private blockchain cloud at a cost. Anyone who subscribes can upload documents to their blockchain and get the documents digitally signed. The user cannot pose as a verified company or agency until they get verified from the site.

These digitally signed documents can then be shared and verified from their site at any time almost instantly. The site will catch any changes occurred in the documents.

While it is a nice implementation, they use a private blockchain to store the documents, which can prove counter-productive shall their database gets attacked.

[2]. A. Gayathiri, J. Jayachitra and S. Matilda “Certification validation using Blockchain”:

In this paper, the authors provide a solution to the same problem as in proposed solution. The paper explains how documents are first turned into digital certificates and then a hash code is generated using chaotic algorithm. These certificates are stored in a private blockchain and in turn can be verified using a mobile application using QR code verification.

However they don’t explain how these certificates can be decentralized as they store it in a private blockchain. They also don’t explain how duplication can be eliminated.

This would lead in a relatively costlier implementation due to the raw computing power required to maintain the blockchain.

[3].Jongbeen Han, Heemin Kim, Hyeonsang Eom, and Yongseok Son. Decentralized Document Management System:

This paper explains how a Decentralized Document Management system can be implemented on a public blockchain. This system would specify user access rights and protects the documents on the blockchain using a symmetric key.

This paper gives an insight as to how documents can be store in a public blockchain.

[4]ipfs.io:

IPFS all in all is a framework as to how decentralized web can work.

From the start of the internet, we have been using HTTP as a world wide format.

HTTP provides a single server multiple clients structure where a single server provides services to multiple client.

IPFS framework ensures faster, more secure internet access through a peer-to-peer connection; at the same time ensuring privacy.

IPFS framework can vastly increase security of documents stored in it by providing a global, secure, and fast access; along with being highly cost effective.

Background Study

Blockchain

Blockchain isn’t a tool, but a technology. It basically a distributed immutable singly link list.

Data on the blockchain is stored in all of the peers containing it; thus providing security. If the data on any block changes, it has to be approved by more than half the peers containing the data. Thus, if an attacker has to change the data, they have to attack half the nodes on the blockchain thus making it highly secure.

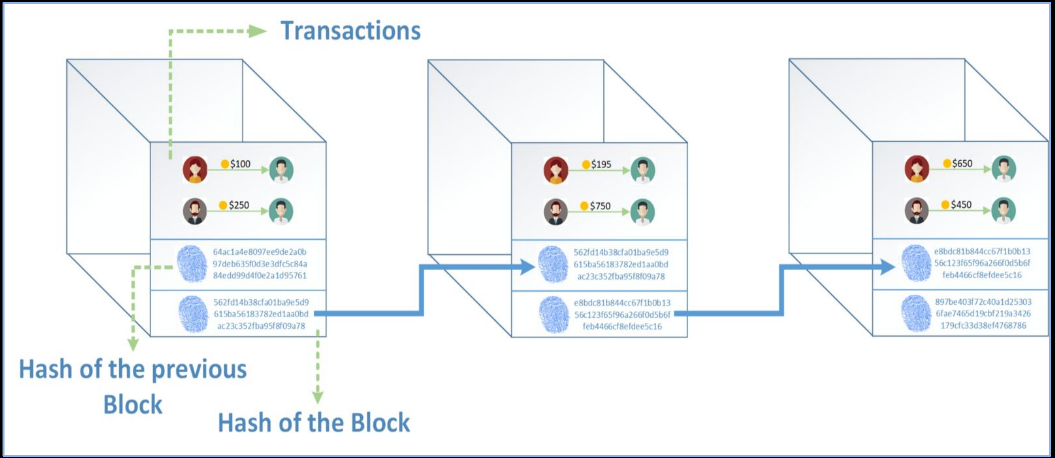
Blockchain Technology | **What is a Blockchain?**

- It is an online ledger that provides decentralized data sharing. It is basically a singly linked list where each block has the hash of its previous block

- As new data comes in it is entered into a fresh block. Once the block is filled with data it is chained onto the previous block

- A Blockchain is not stored on one person’s computer. Instead, it is stored in a large network of computers called a **peer-to-peer** network.

- **Transaction**:represents the action triggered by the participant.

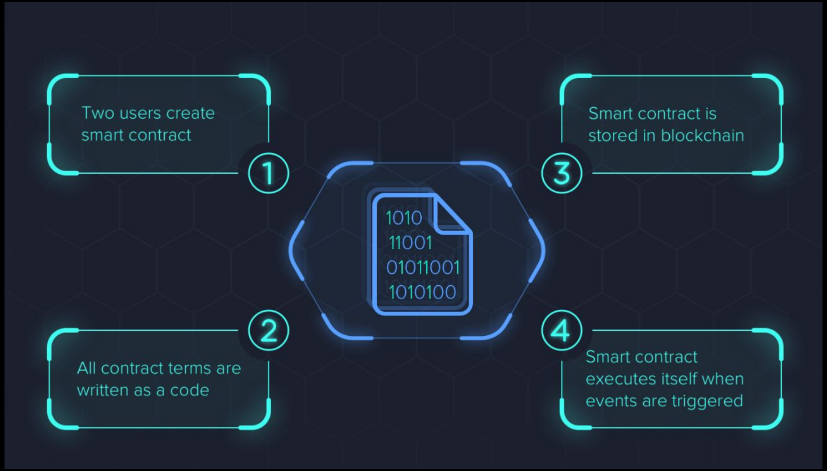


Blockchain Technology | What are Smart Contracts?

- Smart contract is a digital contract that is written in source code and is executed by computers, which integrates the tamper-proof mechanism of blockchain.

- Developers according to their needs are able to specify any instruction in smart contracts, develop various types of applications, including those that can interact with other contracts too, store data and transfer Ethers.

- Smart contracts which are deployed in blockchains are copied to each node to prevent contract tampering.

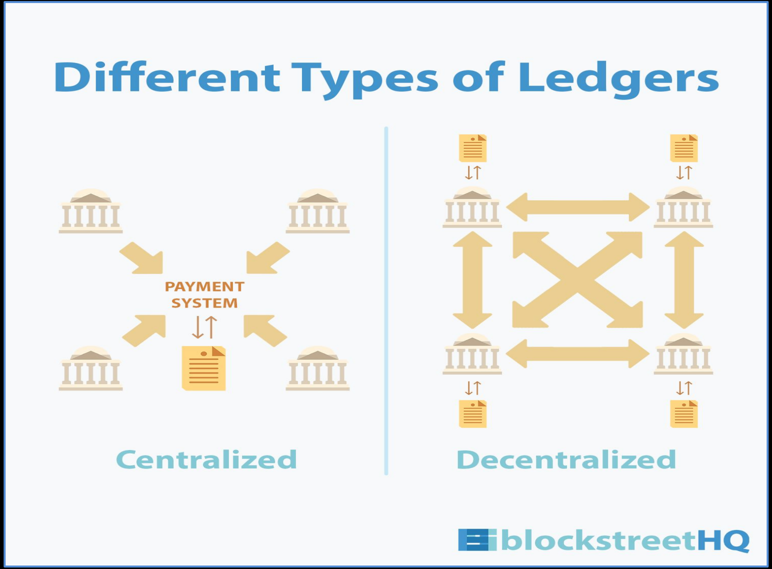

1
Two users create smart contract
2
All contract terms are written as a code
1010
11001
01011001
1010100
3
Smart contract is stored in blockchain
4
Smart contract executes itself when events are triggered

Blockchain Technology | **What are Distributed Ledgers?**

- A distributed ledger is a type of database that is shared, replicated, and synchronized among the members of a decentralized network. It records the transactions, such as the exchange of assets or data, among the participants in the network.

- The need for a central authority to keep a check against manipulation is eliminated by the use of a distributed ledger.

- Every record in the distributed ledger has a timestamp and unique cryptographic signature,which makes the ledger auditable and immutable.



Work Done

In this project we design a DApp (Decentralized Application) which can be used by the University to issue certificates to a public blockchain.

1. User Interface:

   The website contains two parts:

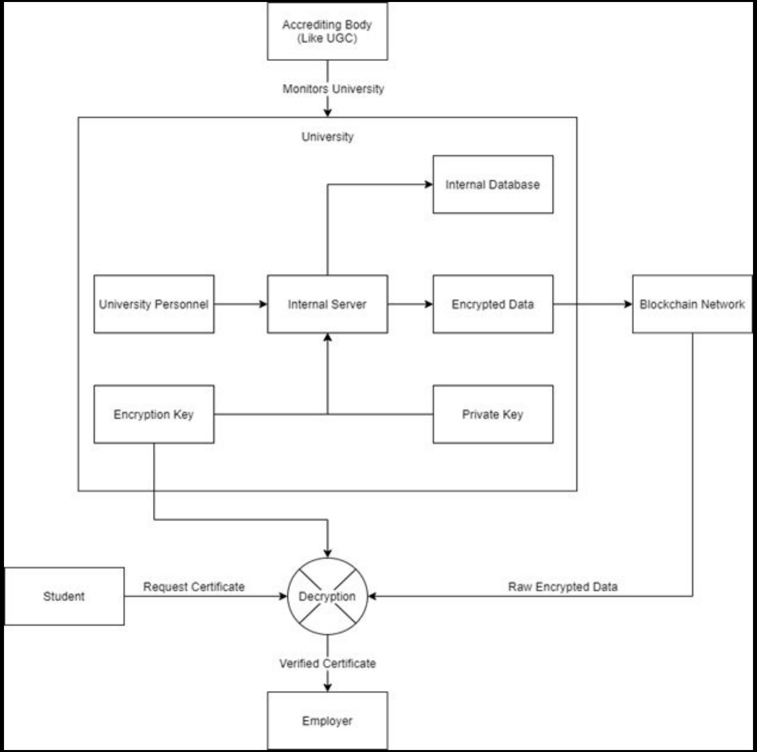
   I. University side: where University issues the certificates by adding student details. The details are read by server and added to the blockchain. The certificate block is created and the previous hash, present hash and timestamp of the issued certificate is returned. The public hash of the block can be used to access and verify the certificates.

   The timestamp with the roll number is broadcasted to all the blocks so that duplication doesn't occur.

II. Student side:

Anyone with the hash value/ student roll number/certificate number can verify the authenticity of the certificate; any fake records/ manipulation in the certificate are readily recognized.

Implementation:



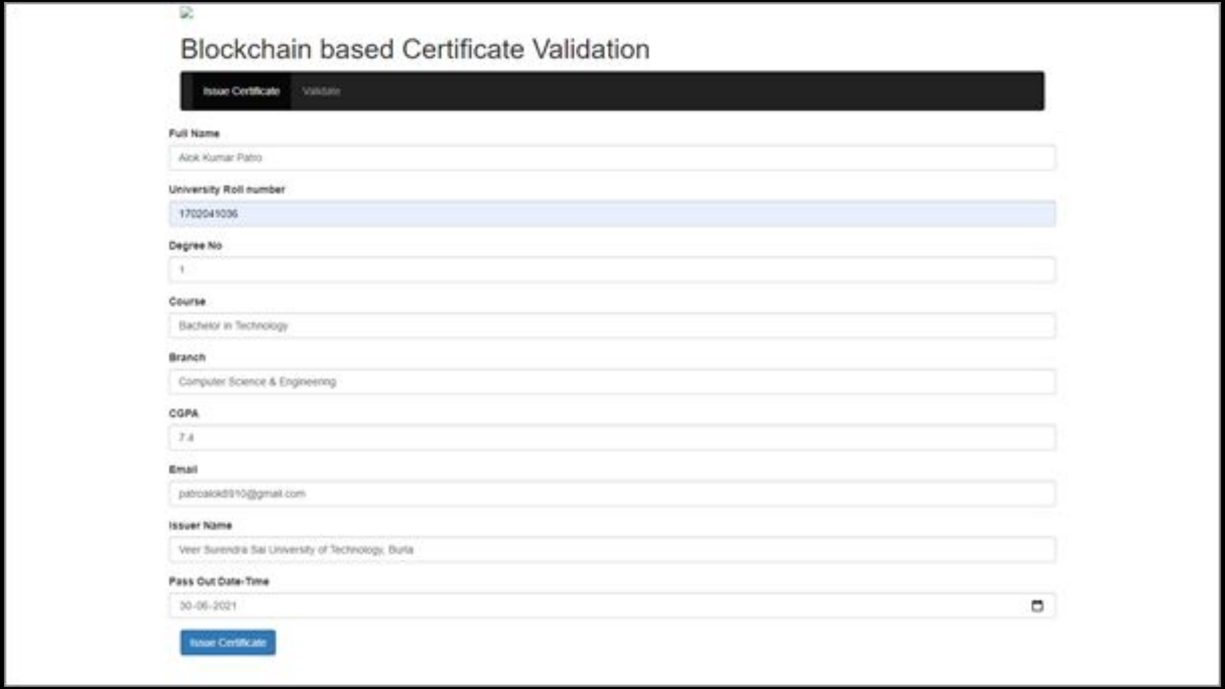
2. Implementation

In the proposed implementation:

- The framework is implemented by a accrediting body such as UGC; UGC monitors the Universities and provides them with verified accounts to access the issuing portal.
- The Universities issue certificates and encrypt them using an AES cipher. The encrypted details are uploaded to the public Ethereum Blockchain and the encryption key is provided to the students.
- Upon requirement, students can use the public hash value of the certificate blocks and the encryption key to access the details of the certificate.
- The same can be done by recruiters to verify the details instantaneously and making the hiring process faster.

Results:

Screenshots:



Blockchain based Certificate Validation

Full Name

Alok Kumar Patro

University Roll number

1702041036

Degree No

1

Course

Bachelor in Technology

Branch

Computer Science & Engineering

CGPA

7.4

Email

patroalok8910@gmail.com

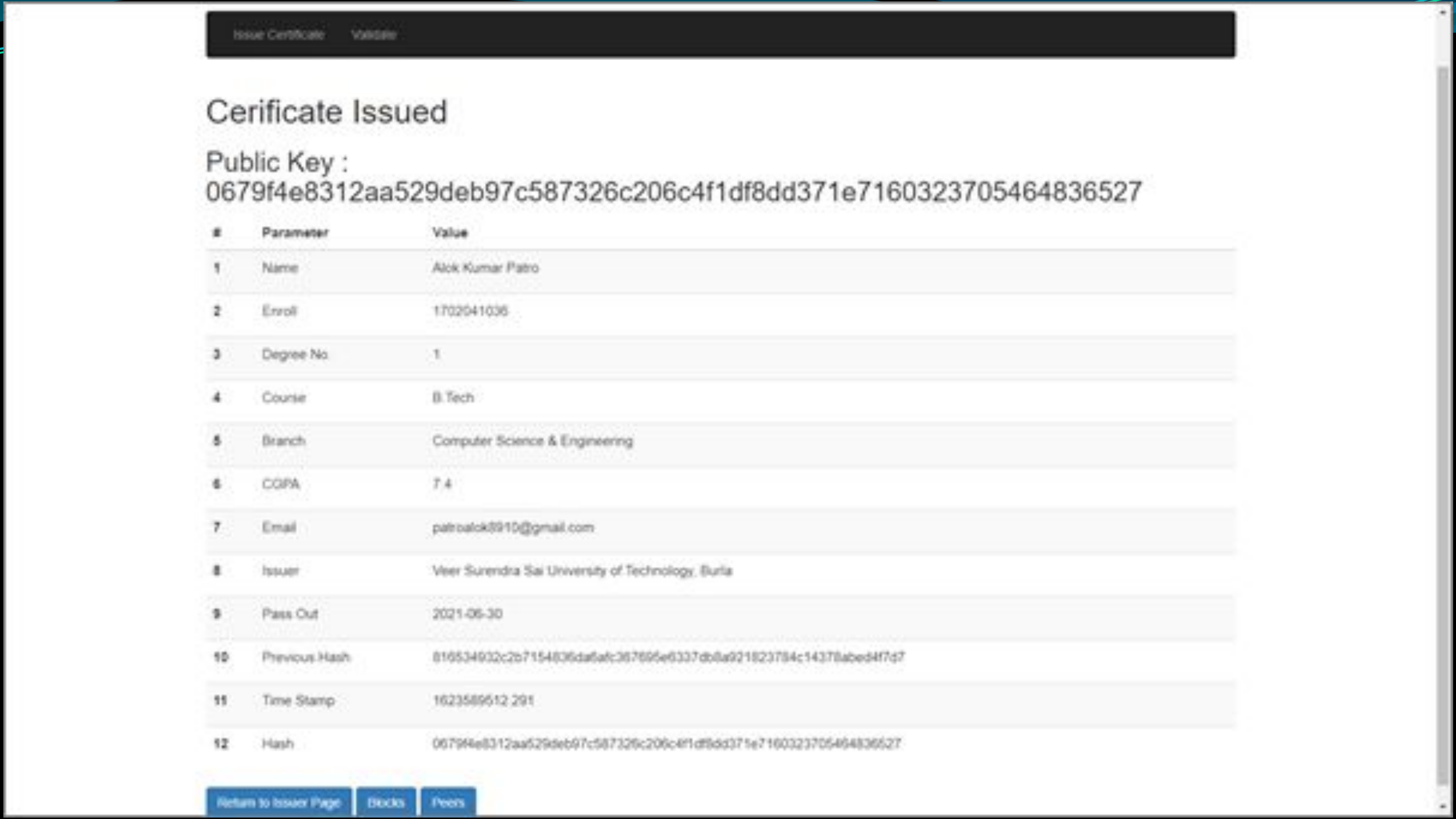
Issuer Name

Veer Surendra Sai University of Technology, Burla

Pass Out Date-Time

30-06-2021

University side site

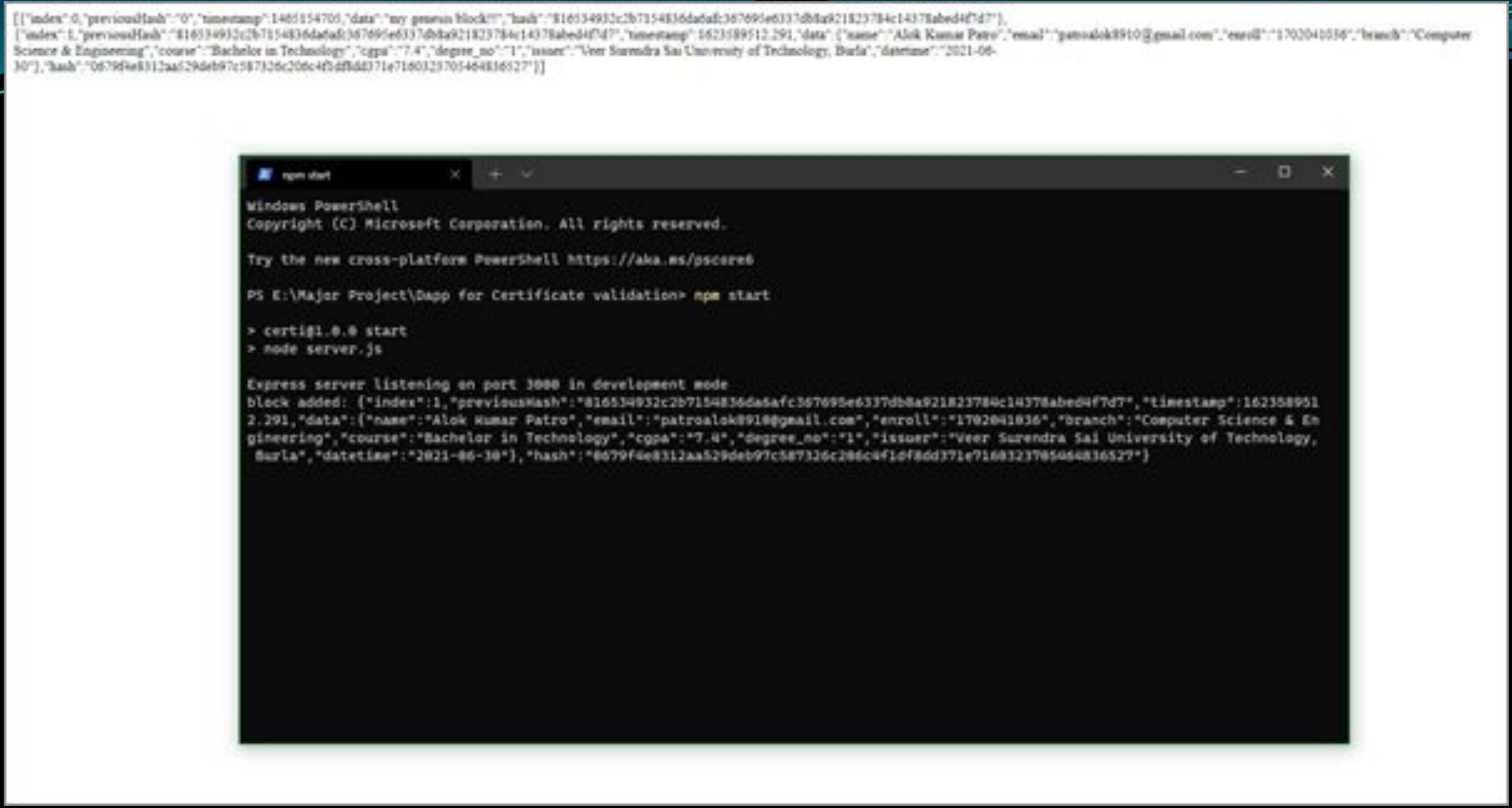


Cerificate Issued

Public Key : 0679f4e8312aa529deb97c587326c206c4f1df8dd371e7160323705464836527

#	Parameter	Value
1	Name	Alok Kumar Patro
2	Enroll	1702041036
3	Degree No	1
4	Course	B.Tech
5	Branch	Computer Science & Engineering
6	CGPA	7.4
7	Email	patroalok8910@gmail.com
8	Issuer	Veer Surendra Sai University of Technology, Burla
9	Pass Out	2021-06-30
10	Previous Hash	816534932c2b7154836da6afc367695e6337db8a921823784c14378abed4f7d7
11	Time Stamp	1623589612.291
12	Hash	0679f4e8312aa529deb97c587326c206c4f1df8dd371e7160323705464836527

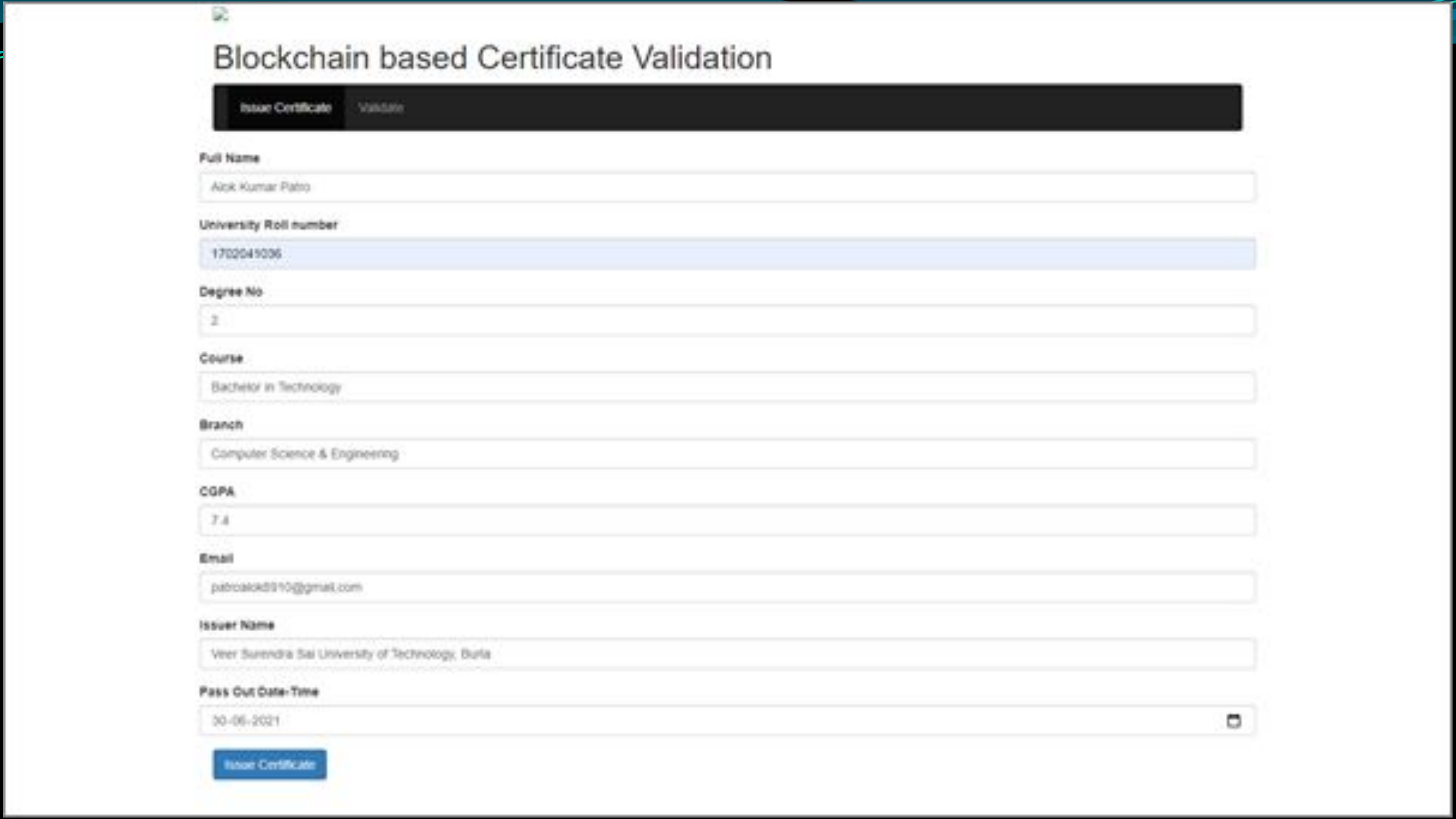
After the Block is added to the blockchain



```
[{"index":0,"previousHash":"0","timestamp":1465154705,"data":"my genesis block!!","hash":"816534932c2b7154836da6afc367695e6337db8a921823784c14378abed4f7d7"},
{"index":1,"previousHash":"816534932c2b7154836da6afc367695e6337db8a921823784c14378abed4f7d7","timestamp":1623589512.291,"data":{"name":"Alok Kumar Patro","email":"patroalok8910@gmail.com","enroll":"1702041036","branch":"Computer
Science & Engineering","course":"Bachelor in Technology","cgpa":"7.4","degree_no":"1","issuer":"Veer Surendra Sai University of Technology, Burla","datetime":"2021-06-
30"},"hash":"0679f4e8312aa529deb97c587326c206c4f1df8dd371e71603237054648365 27"}]
```

```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS E:\Major Project\Dapp for Certificate validation> npm start

> certi@1.0.0 start
> node server.js

Express server listening on port 3000 in development mode
block added: {"index":1,"previousHash":"816534932c2b7154836da6afc367695e6337db8a921823784c14378abed4f7d7","timestamp":162358951
2.291,"data":{"name":"Alok Kumar Patro","email":"patroalok8910@gmail.com","enroll":"1702041036","branch":"Computer Science & En
gineering","course":"Bachelor in Technology","cgpa":"7.4","degree_no":"1","issuer":"Veer Surendra Sai University of Technology,
 Burla","datetime":"2021-06-30"},"hash":"0679f4e8312aa529deb97c587326c206c4f1df8dd371e716032370546483652 7"}
```

(Project in development mode) The added blocks can be seen in the console



Blockchain based Certificate Validation

Full Name

Alok Kumar Patro

University Roll number

1702041036

Degree No

2

Course

Bachelor in Technology

Branch

Computer Science & Engineering

CGPA

7.4

Email

patroalok0910@gmail.com

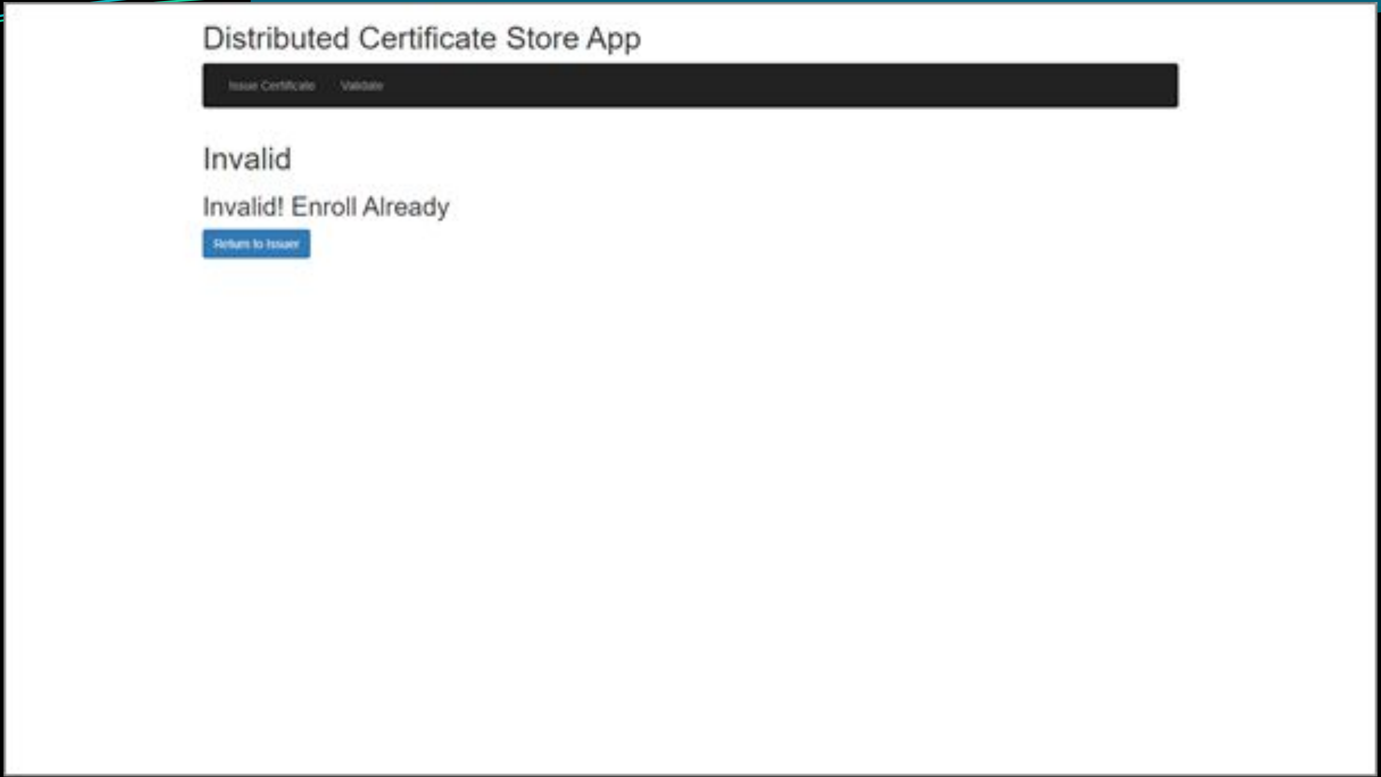
Issuer Name

Veer Surendra Sai University of Technology, Burla

Pass Out Date-Time

30-06-2021

Duplicate entries are not accepted(1)

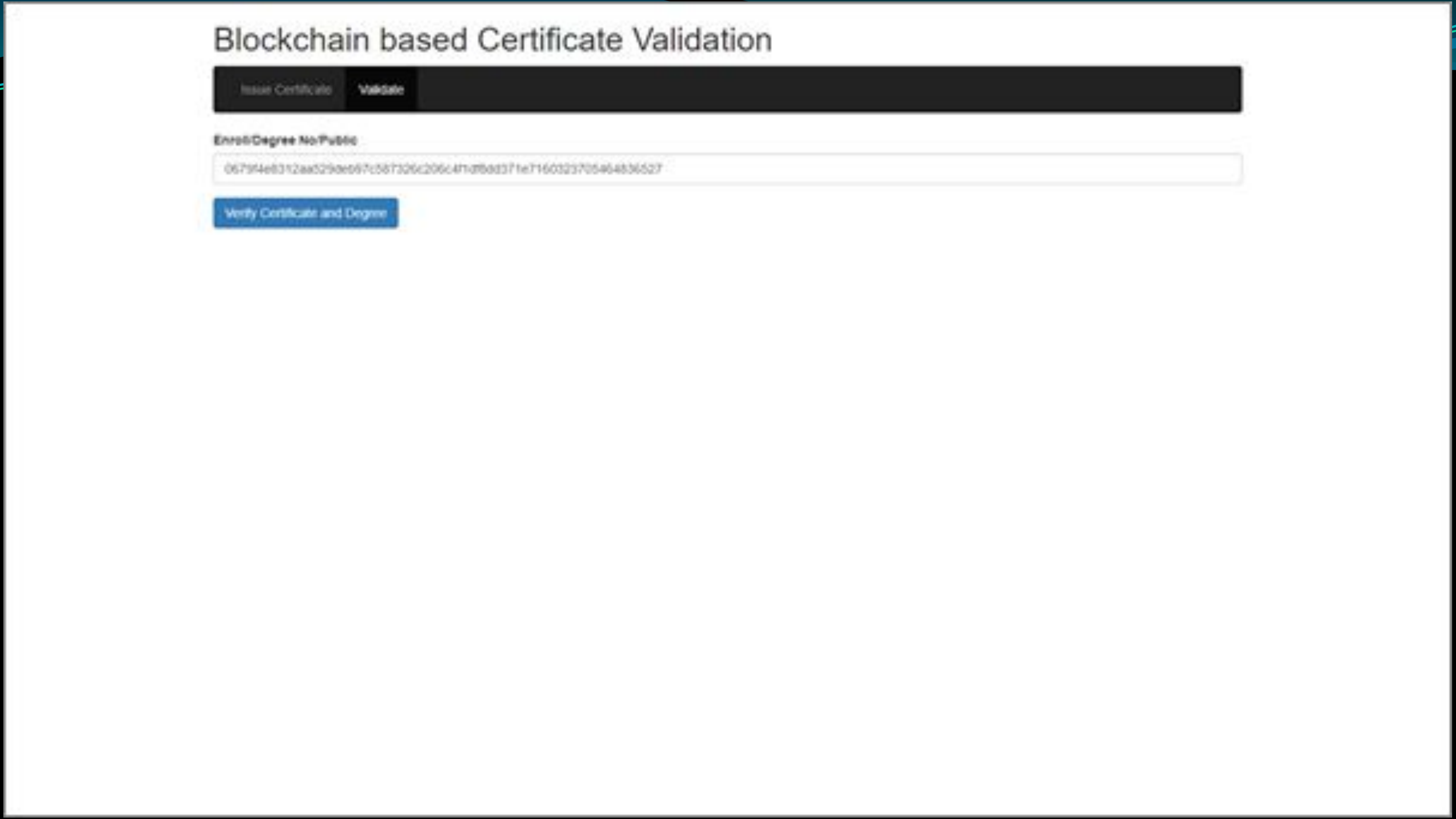


Distributed Certificate Store App

Invalid

Invalid! Enroll Already

Duplicate entries are not accepted(2)

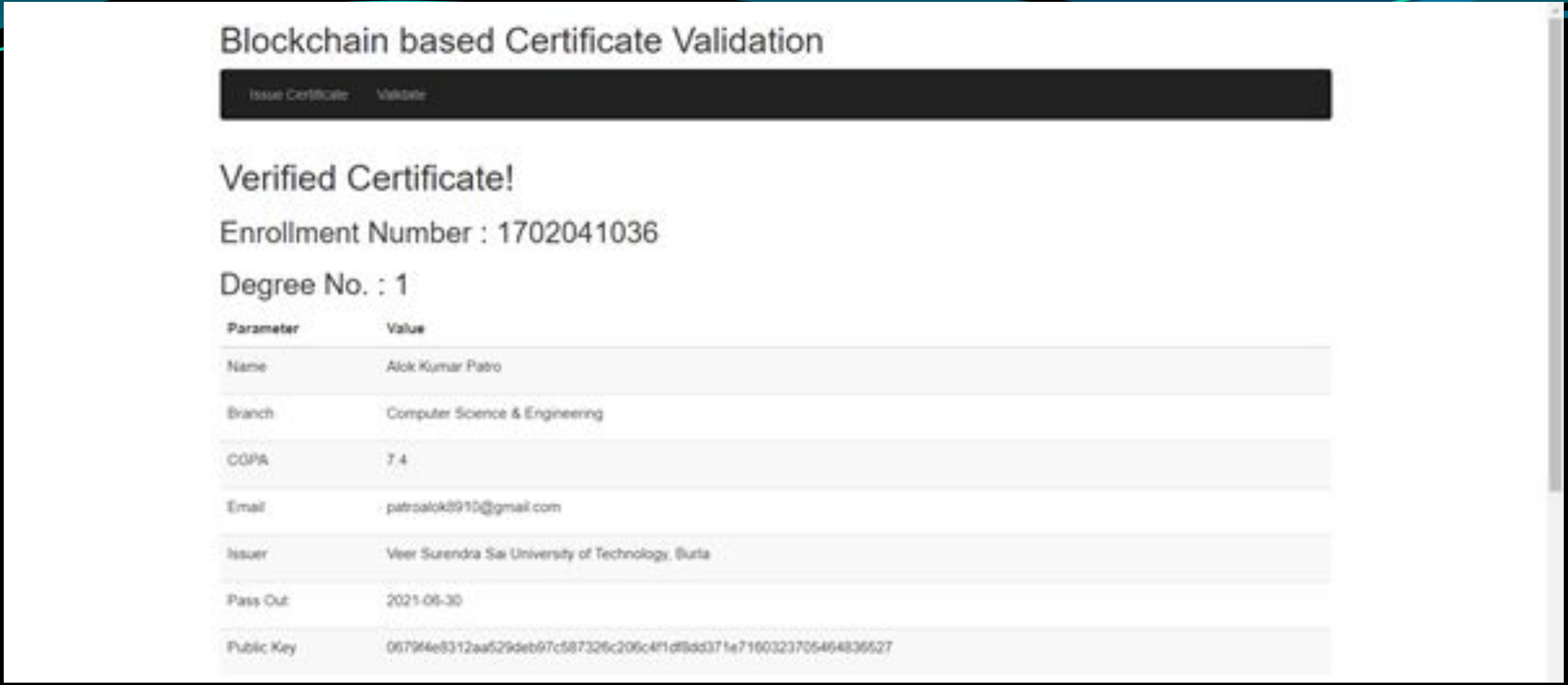


Blockchain based Certificate Validation

Enroll/Degree No/Public

0679f4e8312aa529de697c587326c206c4f1df8dd371e7160323705464836527

Student-side (Verification)



Blockchain based Certificate Validation

Verified Certificate!

Enrollment Number : 1702041036

Degree No. : 1

Parameter	Value
Name	Alok Kumar Patro
Branch	Computer Science & Engineering
CGPA	7.4
Email	patroalok8910@gmail.com
Issuer	Veer Surendra Sai University of Technology, Burla
Pass Out	2021-06-30
Public Key	067964e8312aa529deb97c587326c206c4f1df8dd371e7160323705464836527

Successful verification

Result:

- The proposed solution upon deployment is a fast and secure way to authenticate certificates. It takes 15 seconds in average to add a certificate to the Ethereum blockchain.
- They can be verified upon request almost instantly.
- Duplicate entries are checked by timestamping the certificates.
- The smart contract is hidden thus making the users and the data on blockchain hidden.
- The solution is pretty cost effective and versatile solution to the existing problem.

Conclusion

The proposed solution can highly benefit students and employers to make verification of documents faster and easier than the existing solution. It'll also reduce manipulation and other unethical practices with educational certificates.

This solution will not only benefit university certificates, but the same framework can be extended to other important documents, exclusive products, loans, etc.

While blockchain technology is still pretty new, significant work is being carried out to make blockchains even more closer to reality.

In present day it is not too cost effective to add data to blockchain, but with gradual advancement in technology and computing power, blockchain is slowly but steadily making way into our daily lives.

Future Scope:

- An IPFS storage can be implemented to ensure global peer-to-peer access to the documents rather than relying on the university hosted site for verification.
- Alternatively the hash code can be QR coded and added to the certificate along with an android application for the student side verification to make verification easier on the go.
- While the dissertation doesn't explain the encryption of files, the encryption of larger documents should be done using a reliable encryption AES algorithm to ensure security of data.

THANK YOU!!

References:

1. Certifaction.io
2. A. Gayathiri, J. Jayachitra and S. Matilda, "Certificate validation using blockchain," 2020 7th International Conference on Smart Structures and Systems (ICSSS), 2020, pp. 1-4, doi: 10.1109/ICSSS49621.2020.9201988
3. Jongbeen Han, Heemin Kim, Hyeonsang Eom, and Yongseok Son. 2021. A decentralized document management system using blockchain and secret sharing. In Proceedings of the 36th Annual ACM Symposium on Applied Computing (SAC '21). Association for Computing Machinery, New York, NY, USA, 305–308. DOI:https://doi.org/10.1145/3412841.3442077
4. IPFS (ipfs.io) – A real world peer-to-peer hypermedia protocol – i.e. a decentralized storage network.