Generating E-Certificate and Validation using Blockchain

[1]Rohan Hargude, [2]Ghule Ashutosh, [3]Abhijit Nawale, [4]Pro.Sharad Adsure

[1,2,3]B.E Students, [4]Professor Comp. Department.

[1,2,3,4]Computer Department, Pune, India.

Abstract: Lakhs of people getting Degrees year after year, due to the lack of effective anti-forge mechanism, events that cause the graduation certificate to be forged often get noticed. according to the Indian Ministry of Education statistics,document certific of of document verification is a complex domain that involves various challenging and tedious processes to authenticate. Certificate of Blockchainis a large and open-access online ledger in which each node saves and verifies the same data. Using the praposed system manual proposed blockchain based system reduces the Likehood of certificate forgery. The process of genartion certificate granting are open and transparent in the system.Due to the lack of an effective anti-forge mechanism, events that cause the graduation certificate to be forged often get noticed.In order to solve the problem of counterfeiting certificates, the digital certificate system based on blockchain technology would be proposed. For students, educational certificates are the most important documents issued by their universities. However, as the issuing process is not that transparent and verifiable, fake certificates can be easily created. A skillful generated fake certificate is always hard to detect and can be treated as the original. With the increase of forged documents, the credibility of both the document holder and the issuing authority is jeopardized. In order to solve the problem of counterfeiting certificates,the digital certificate system based on blockchain technology would be proposed. By the modifiable property of blockchain, the digital certificate with anti-counterfeit and verifiability could be made. The procedure of issuing the digital certificate a in this system is as follows. First, generate the electronic file of a paper certificate accompanying other related data into the database, meanwhile, calculate the electronic file for its hash value. Finally, store the hash value into the block in the chain system. In this research, the authors have identified the security themes required for document verification in the blockchain.This research also identifies the gaps and loopholes in the current blockchain-based educational certificate verification. The system will create a related QR-code and inquiry string code to affix to the paper certificate. It will provide the demand unit to verify the authenticity of the paper certificate through mobile phone scanning or website inquiries.

Keywords :E-Certificate,Blockchain,Smart Contract,Metamask

A: Background Information:

Maharashtra went through a few vacillations last year as for the retail cost of onions. The cost expanded from Rs. 26 foreach kiloin the primary portion of the year to an incredible Rs. 50 for every kilo in August. Noticing the shoot in the value,a considerable lot of the ranchers in the state chose to develop onions on their homestead, in the expectation of making Advances in information technology, the wide availability of the Internet, and common usage of mobile devices have changed the lifestyle of human beings. Virtual currency, digital coins originally designed for use online, has begun to be extensively adopted in real life. Because of the convenience of the Internet, various virtual currencies are thriving, including the most popular—Bitcoin, Ether, and Ripple [2]—the value of which has surged recently. People are beginning to pay attention to blockchain, the backbone technology of these revolutionary currencies. Blockchain features a decentralized and incorruptible database that has high potential for a diverse range of uses. Blockchain is a distributed database that is widely used for recording distinct transactions. Once a consensus is reached among different nodes, the transaction is added to a block that already holds records of several transactions. Each block contains the hash value of its last counterpart for connection. Blockchain is a distributed database that is widely used for blockchain [1]. Data are distributed among various nodes (the distributed data storage) and are thus decentralized. Consequently, the nodes maintain the database together. Under blockchain, a block becomes validated only once it has been verified by multiple parties. Furthermore, the data in blocks cannot be modified arbitrarily. A blockchain-based smart contract, for example, creates a reliable system because it dispels doubts about information's veracity.

B : Rational:

 Because information technology has developed rapidly in recent years, data protection is more necessary than ever. Graduates, whether they choose to continue studying or start job hunting, require various certificates for interviews. they often find that they have lost their educational and commendation certificates. Reapplying for hard copies can be time-consumingbecause certificates are granted by different organizations and in-person application may be necessary. By contrast, applying for an e-copy can save paper and time. By providing information for identity verification, graduates are able to apply for any certificate easily. Nevertheless, because of this convenience, forged degree certificates,licenses.
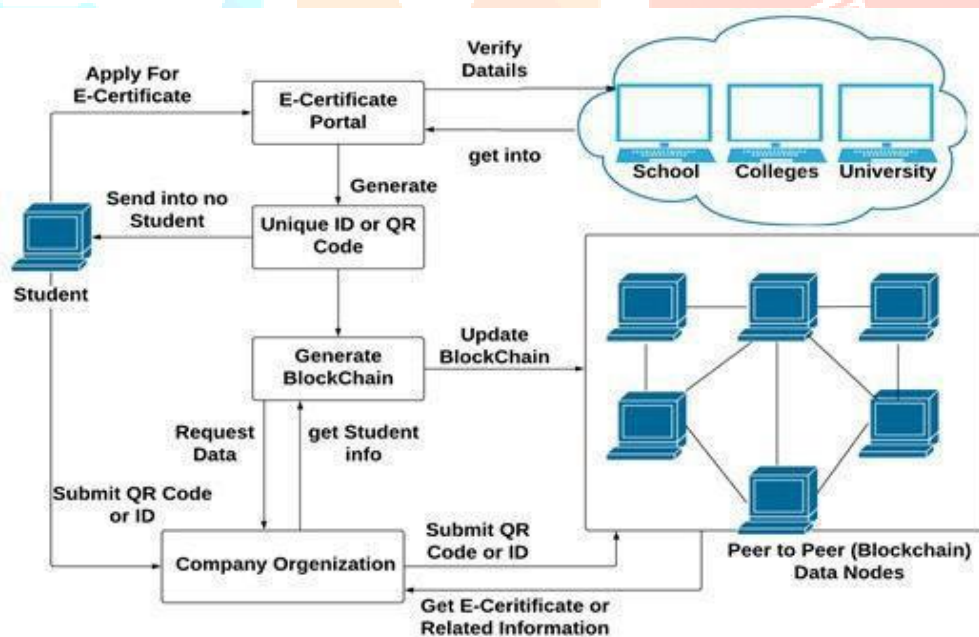
Blockchain:

The concept of blockchain was proposed by Satoshi Nakamoto in 2008. Blockchain is an online ledger that provides decentralized and transparent data sharing. With distributed recordings, all transaction data (stored in nodes) are compressed and added to different blocks.Data of various types are distributed in distinct blocks, enabling verifications to be made without the use of intermediaries. All the nodes then form a blockchain with timestamps. The data stored in each block can be verified simultaneously and become inalterable once entered. The whole process is open to the public, transparent, and secure [8].The emergence of Ethereum Smart Contracts in 2013

boosted blockchain technology, which became blockchain 2.0. As presented in Fig. 1, blockchain 1.0 was mainly adopted by Bitcoin to solve problems concerning cryptocurrencies and decentralized payments.Blockchain 2.0 focused on decentralizing the entire market and is employed to transform assets through smart contracts, thereby creating value through the emergence of alternatives to Bitcoin Blockchain.
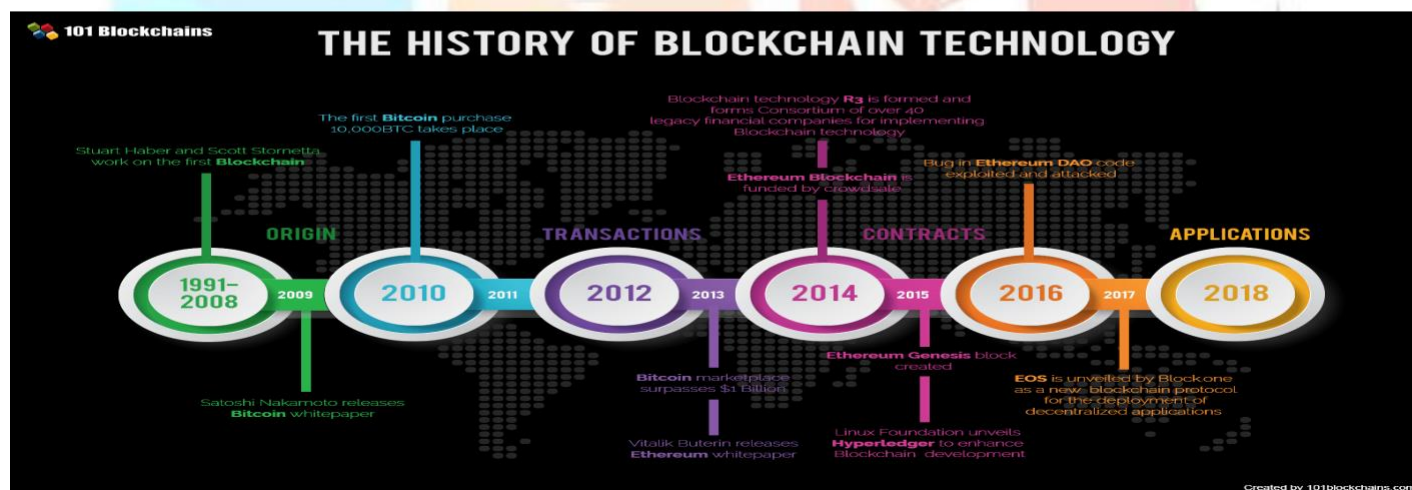
SYSTEM ARCHITECTURE

WORKING PROCESS

Blockchain is a decentralized distributed database. The working processes of the system developed in this study are as follows:

Schools grant a degree certificate and enter the student's data into the system. Next, the system automatically records the serial number of the student in a blockchain. The certificate system verifies all the data.Instead of sending conventional hard copies, schools grant e-certificates containing a quick response (QR) code to the graduates whose data have been successfully verified. Each graduate also receives an inquiry number and electronic file of their certificate.When applying for a job, a graduate simply sends the serial number or e-certificate with a QR code to the target companies.The companies send inquiries to the system and are informed if the serial numbers are validated. The QR code enables them to recognize if the certificate has been tampered with or forged.

OPRATIONS:

E-certificate generation system which manually creates the certificates based on current students data. Various centralized methods follow the similar approach for verification. The entralized approaches cant defend the various network attacks like SQL injection, Collusion,bruited force etc. Blockchain approach using decentralized approach. Fog computing or fognetworking, also known as fogging, is pushing frontiers of computing applications, data, and services away from centralized cloud to the logical stream of the network edge. Fog networking system works on to build the control, configuration, and management over the Internet backbone rather

than the primarily control by network gateways and switches those which are embedded in the LTE network. We can illuminate the fog computing framework as highly virtualized computing infrastructure which provides hierarchical computing facilities with the help of edge server nodes. These fog nodes organize the wide applications and services to store and process the contents in close proximity of end users.

DEVELOP ARCHITECTURE:

All the nodes then form a blockchain with timestamps. The data stored in each block can be verified simultaneously and become inalterable once entered. The whole process is open to the public, transparent, and secure [8].The emergence of Ethereum Smart Contracts in 2013 boosted blockchain technology, which became blockchain 2.0. As presented in , blockchain 1.0 was mainly adopted by Bitcoin to solve problems concerning cryptocurrencies and decentralized payments.Blockchain 2.0 focused on decentralizing the entire market and is employed to transform assets through smart contracts, thereby creating value through the emergence of alternatives to Bitcoin .
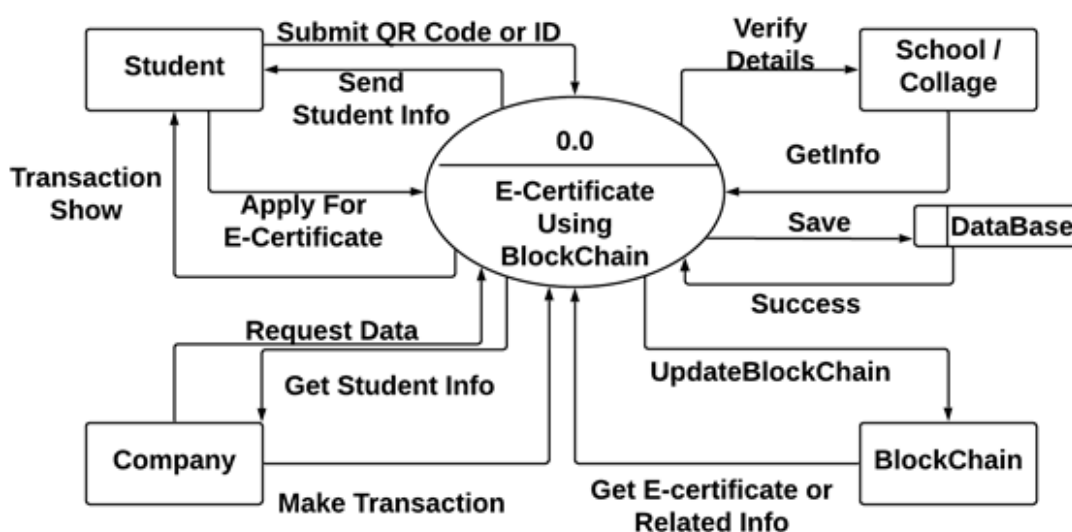
List of Modules and Functionality:

System proposed a new dynamic certificate generation approach using own custom blockchain. First student apply for e-certificate on web portal with upload all educational documents.Web portal is authenticate trusted third party which validate all documents from university, school, colleges etc. Once successfully verification has done from university, school, colleges it will store data into blockchain and same time it generates the unique certificate id or QR code and returns to student. Student can submit the received QR code or certificate id to organization instead of physical hard copy of documents. Organization can submit QR code or id to portal and pool the e-certificate of respective student and make the validation. The entire process has perform into the blockchain manner with smart contract which is written by us. To execute the system in vulnerable environment and to explore and validate how proposed system eliminate different network attacks like DOS and MiM.

Dynamic QR-code andunique certificate generation for each students document in proposed system. Data e-certificate stored into the blockchain in secure Manner which enhance the security. According to the smart contract system also allow the updates in entire blockchain.This research proposed a custom blockchain generation on open source platform.

TOOLS AND TECHNOLOGIES USED :

1)VS CODE:

Visual Studio Code is a streamlined code editor with support for development operations like debugging, task running, and version control. It aims to provide just the tools a developer needs for a quick code-build-debug cycle and leaves more complex workflows to fuller featured IDEs, such as Visual Studio IDE.The code of the editor is completely Open Source, and there's no payment required to use it. It uses Electron as its base, which enables it to be cross platform and work on Mac, Windows and Linux. It's built using Node. js, and you can extend it using JavaScript (which makes it a win for all us JavaScript developers

2)REACT JS :

React is a library for building composable user interfaces. It encourages the creation of reusable UI components, which present data that changes over time. Lots of people use React as the V in MVC. React abstracts away the DOM from you, offering a simpler programming model and better performance. React can also render on the server using Node, and it can power native apps using React Native. React implements one-way reactive data flow, which reduces the boilerplate and is easier to reason about than traditional data binding.

3)ETHEREUM:

Ethereum is a blockchain platform with its own cryptocurrency,called Ether (ETH) or ethereum, and its own programming language, called Solidity. As a blockchain network, ethereum is a decentralized public ledger for verifying and recording transactions. Its cryptocurrency is now second only to Bitcoin in market value.It is the fuel that runs the network. It is used to pay for the computational resources and the transaction fees for any transaction executed on the ethereum network. Like Bitcoins,ether is a peer-to-peer currency. Apart from being used to pay for transactions, ether is also used to buy gas, which is used to pay for the computation of any transaction made on the ethereum network.

Deployment
Educational documents verification is very tedious and time consuming process in real time environment. E- Certificate generation for entire educational history is easy process to eliminate such consuming tasks.
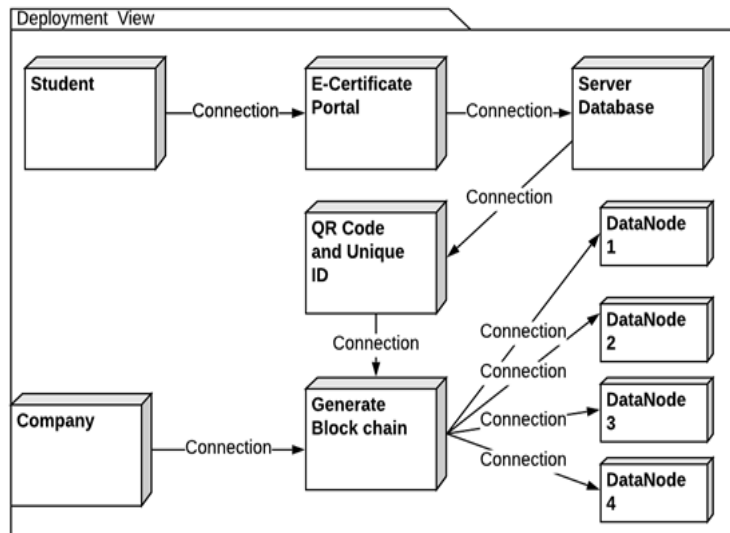

TESTING :
Along with the type of testing also mention the approach to be followed for the testing, that is, Manual Testing or Automated Testing.Use Automated Testing Plan forplanning automation activities in details. The different types of testing that may be carried out in the project Are as follows Individual components are tested independently to ensure their quality.The focus is to uncover errors in design and implementation. ata structure in component rogram logic and program structure in a component Component interface *f*unctions and operations of a component.

System Testing :
The system software is tested as a whole. It verifies all elements mesh properly to make sure that allsystem functions and performance are achieved in the target environment.
The focus areas are: System functions and performance System reliability and recoverability (recovery test) System behavior in the special conditions (stress and load test)   System user operations (acceptance test/alpha test)   Hardware and software integration collaboration Integration of external software and the system.

Validation Testing:
Validation can be defifined in many ways, but a simple defifinition is that succeeds when software functions in a manner that can be reasonably expected by the customer. Software validation is achieved through a series of black-box tests that demonstrate conformity with requirements. A test plan outlines the classes of tests to be conducted and a test procedure defifines specifific test cases that will be used the demonstrate conformity with requirements. Both the plan and procedure are designed to ensure that all functional requirements are satisfified, all behavioral characteristics are achieved, all performance requirements are attained, documentation is correct, and human engineered and other requirements are met.

Integration Testing :
A group of dependent components are tested together to ensure their Quality of their integration unit. This approach is to do incremental integration to avoid bigbang problem. That is when the entire programs put together from all units and tested as a whole. The big-bang approach usually results in chaos which incremental integration avoids. Incremental integration testing can be done in two different way top down and bottom up. Then there is also the possibility of regression integration. The top down integration is when modules are integrated by moving downwards through the control hierarchy, beginning with the main control module. Modules subordinate to the main control module are incorporated into main structure n either depth-fifirst or breadth-fifirst manner.

RESULTS:

SCREENSHORTS:
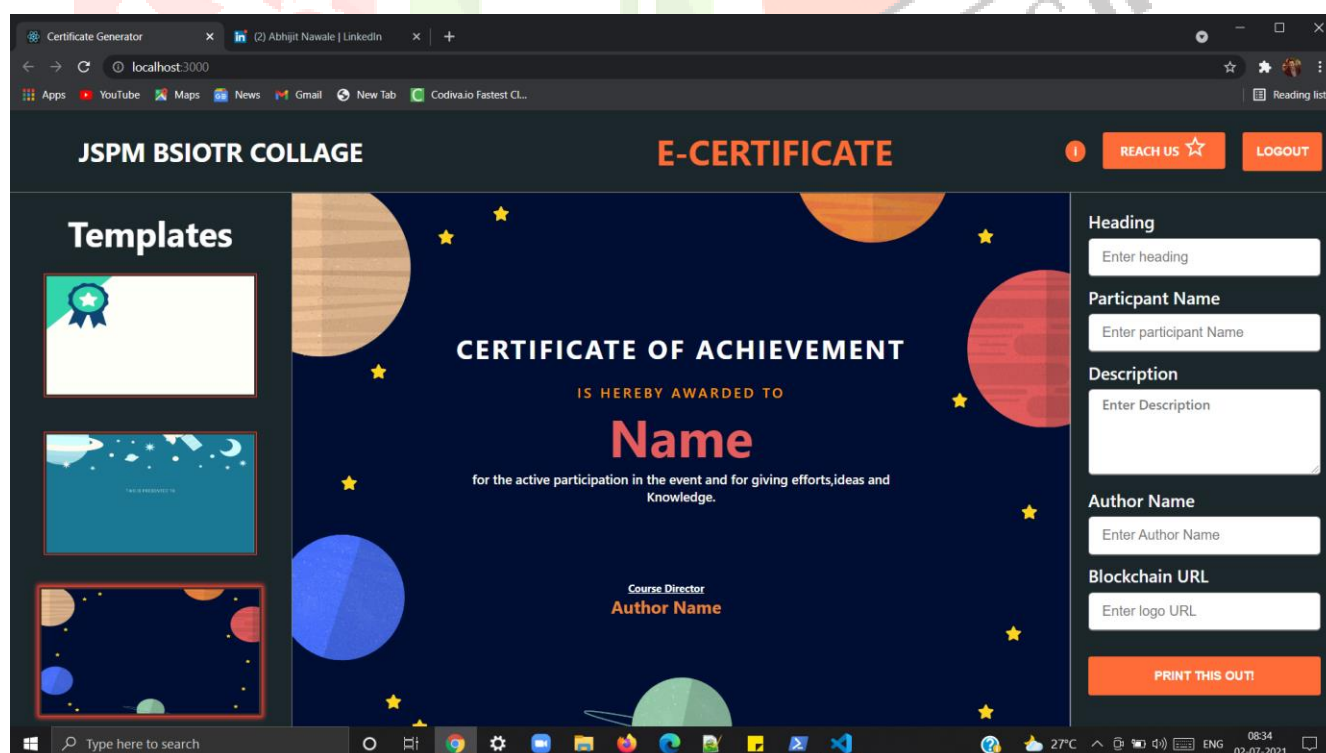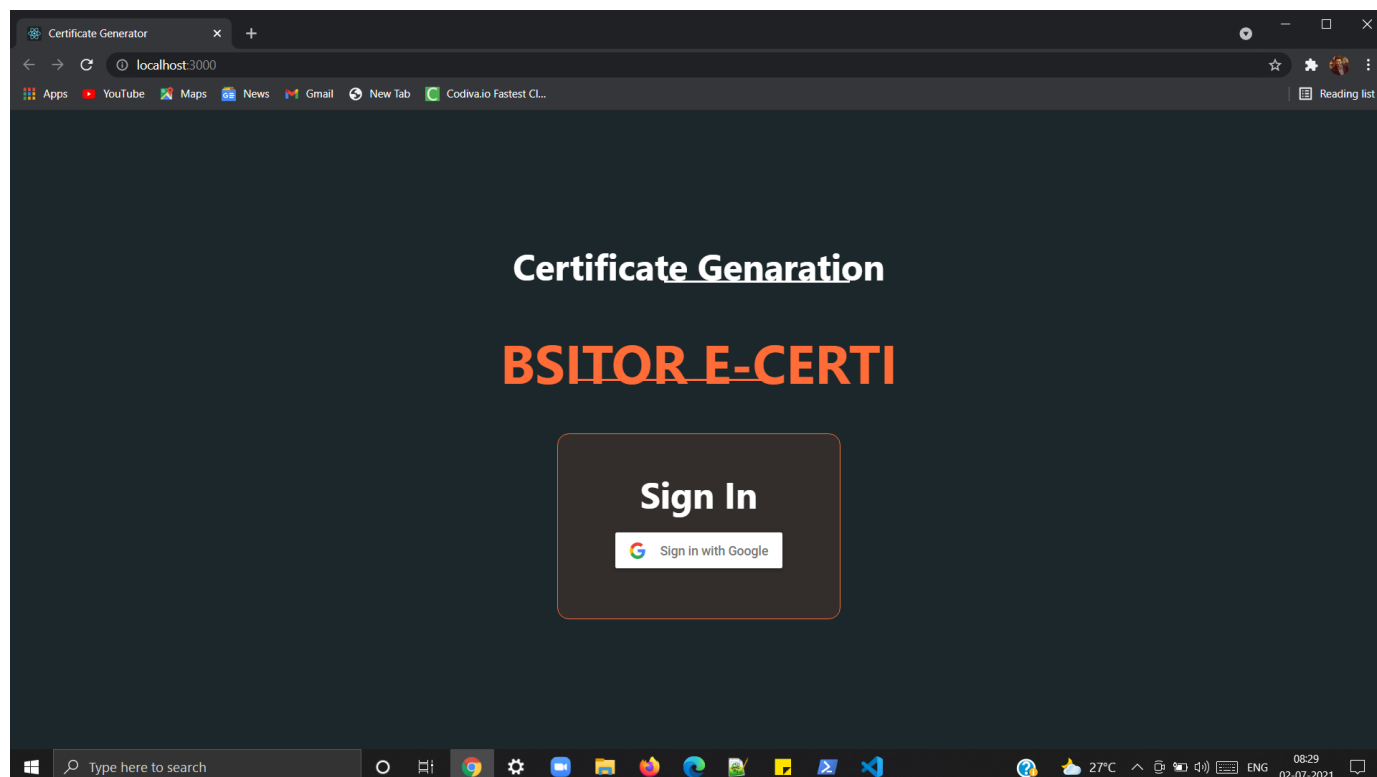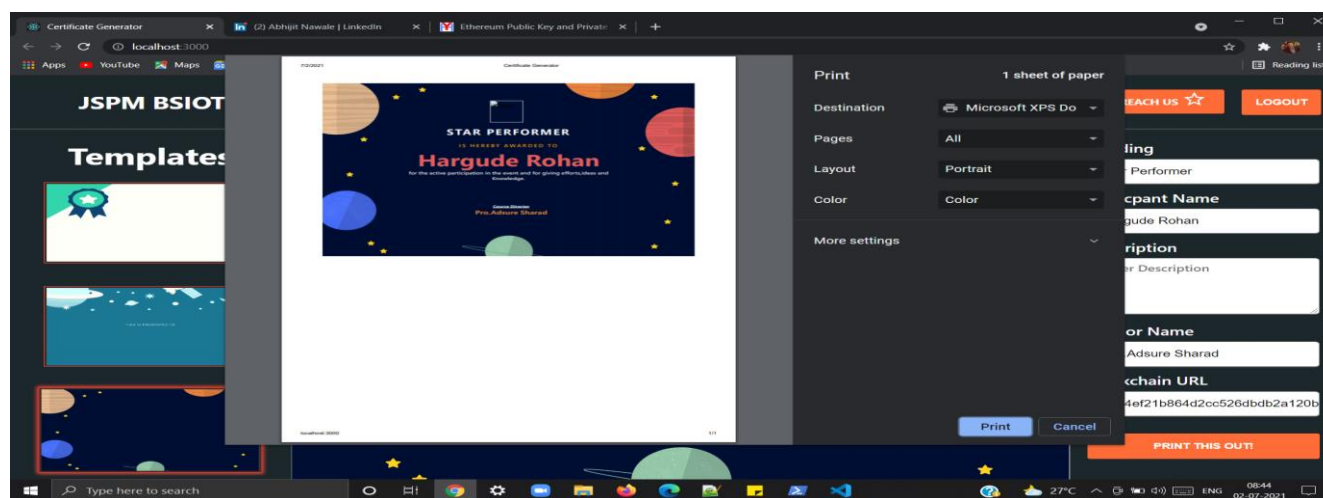
OUTCOMES:

To create the blockchain based unmodifiable certificates, initially the university needs to get registered.

Any transaction can be sent through the wallet address of the Registered university. Only the owner of the smart contract has the authority to add the universities.Once added the university, will be able to access the system and can create Certificates with data fields. Each created certificate will be stored in the Inter planetary file system (IPFS). It will then return the unique hash generated using SHA-256 algorithm.This will serve as unique identity for each document his generated hash and detail of certifi-cates will be stored in the blockchain and the student will be provided with the resultant transaction id. Anyone can use this transaction id to verify the certificate details and can view the original copy of certificate using IPFS hash stored along with data. And it is not using the same data. Hence with this we can solve the problem of certificate frogery.

CONCLUSION :

Data security is one of the major features of blockchain technology. Blockchain is a large and open-access online ledger in which each node saves and verifies the same data.Using the proposed blockchain-based system reduces the likelihood of certificate forgery. The process of certificate application and automated certificate granting are open and transparent in the system. Companies or organizations can thus inquire for information on any certificate from the system. In conclusion, the system assures information accuracy and security.

REFERENCE :

1]Tengyu Yu, Blockchain operation principle analysis: 5 key technologies, iThome.

2] Jingyuan Gao, The rise of virtual currencies! Bitcoin takes the lead, and the other 4 kinds can't be missed. Digital Age.

3] Smart contracts whitepaper,
   https://github.com/OSE-Lab/learning-blockchain/blob/ master/ethereum/smart-contracts.md

4] Gong Chen, Development and Application of Smart Contracts,
   https://www.fisc.com.tw/Upload/b0499306-1905-4531- 888a-2bc4c1ddb391/TC/9005.pdf

5] Weiwei He, Exempted from cumbersome auditing and issuance procedures, several national junior diplomas

6] Xiuping Lin, "Semi-centralized Blockchain Smart Contracts:

7] Solidity   https://solidity.readthedocs.io/en/latest/index.html