

A

Dissertation On

“Digital Certificate by Blockchain Technology”

Submitted in Partial Fulfilment of the Requirement
For the Award of Degree of

Master of Technology

In

Software Technology

By

Sumit Garg

University Roll No. 2K14/SWT/514

Under the Esteemed Guidance of

Dr. Kapil Sharma

HOD, Department of Information Technology, DTU



**COMPUTER SCIENCE & ENGINEERING DEPARTMENT
DELHI TECHNOLOGICAL UNIVERSITY
DELHI – 110042, INDIA**

STUDENT UNDERTAKING



Delhi Technological University
(Government of Delhi NCR)
Bawana Road, New Delhi-42

This is to certify that the thesis entitled “**Digital Certificate by Blockchain Technology**” done by me for the Major Project for the award of degree of **Master of Technology** Degree in **Software Engineering** in the **Department of Computer Science & Engineering**, Delhi Technological University, New Delhi is an authentic work carried out by me under the guidance of Dr. Kapil Sharma.

Signature:

Student Name: Sumit Garg

Roll No: 2K14/SWT/514

Above Statement given by Student is Correct.

Project Guide: Dr. Kapil Sharma

Head of Department

Department of Information Technology

Delhi Technological University, Delhi

ACKNOWLEDGEMENT

I take this opportunity to express my deep sense of gratitude and respect towards my guide **Dr.Kapil Sharma, Head of Department, Department of Information Technology.**

I am very much indebted to him for his generosity, expertise and guidance that I have received from him while working on this project. Without his support and timely guidance the completion of the project would have seemed a far-fetched dream. In this respect I find myself lucky to have my guide. He have guided not only with the subject matter, but also taught the proper style and techniques of documentation and presentation. I would also like to take this opportunity to present my sincere regards

Dr. Ruchika Malhotra, Assistant Professor, DTU for extending their support and valuable Guidance.

Besides my guide, I would like to thank entire teaching and non-teaching staff in the Department of Computer Engineering, DTU for all their help during my tenure at DTU. Kudos to all my friends at DTU for thought provoking discussion and making stay very pleasant.

SUMIT GARG

M.Tech, Software Engineering

2K14/SWT/514

ABSTRACT

As education becomes more diversified, decentralized and democratized, we still need to maintain reputation, trust in certification and proof of learning. Nowadays everyone has to show his/her Document and Certificate to any other person for some purpose/job. After seeing the document 3rd person cannot validate the originality of the certificate.

The same thing is applied for a land registry, PAN card, and Aadhar card verification. The increased focus on relevance and employability may also push us in this direction, as we also need more transparency. We can solve this problem or get trust by using blockchain technology.

The digital currency Bitcoin is probably the best known application of blockchain and is even better known than the Blockchain technology on which it is based [1]. The blockchain is a chain of blocks and blocks are immutable in a distributed environment, in which storage devices are not all connected to a common processor. It is a database of records/public ledger of all transactions /digital events that have been performed and information is shared within participating parties. Each entry in the system is verified by common consent of the participants in the system. Once information is entered in blockchain it cannot be erased. It could provide a system that is transparent and secure. Blocks (Ordered Records) are added to blockchain with timestamp and a link to a previous block.

Verifying a diploma/certificate today takes a good amount of time and requires human resources or human resources to request confirmation of details from universities. A possible solution is Blockchain; Blockchain for education may be a new concept. By using this technology,

No need for a central authority to validate certificates. Your college won't have to send you a copy of your transcript and prove to anyone you have your degree

We are building a platform that will be open, accessible and one piece of software at a time and students can get Blockchain-based educational certifications. Blockchain-based educational certifications are the digital certificate and registered on the Ethereum Blockchain that will be cryptographically signed and tamper proof). Another person can view the certificate online, and no 3rd party validation is required for these digital certificates.

TABLE OF CONTENTS

CERTIFICATE.....	ii
ACKNOWLEDGEMENT.....	iii
ABSTRACT.....	iv
TABLE OF CONTENTS	vi
LIST OF FIGURES	viii
LIST OF TABLES	viii
CHAPTER 1	
INTRODUCTION.....	1
1.1. GRENRAL CONCEPTS	1
1.2. MOTIVATION.....	2
1.3. RELATED WORK	4
1.4. PROBLEM STATEMENT	7
1.5. SCOPE OF THE THESIS.....	8
CHAPTER 2	
LITERATURE SURVEY.....	9
2.1. BLOCKCHAIN	9
2.2. BLOCKCHAIN WORKING	11
2.3. PUBLIC AND PRIVATE BLOCKCHAIN	13
2.4. CRYPTOCURRENCY	14
CHAPTER 3	
PROPOSED WORK.....	16
3.1. DIGITAL CERTIFICATE GERNEARTION.....	16
3.2. PROPOSED MODEL	17

CHAPTER 4

PROPOSED METHODOLOGY..... 18

4.1. SMART CONTRACTS 18

4.2. THE ETHEREUM VIRTUAL MACHING 19

4.3. GAS..... 19

CHAPTER 5

EXPERIMENTS & RESULTS..... 20

5.1. TOOLS USED 20

5.2. RESULTS..... 25

CHAPTER 6

CONCLUSION 28

REFERENCES..... 29

LIST OF FIGURES

Figure 1.1: Blockchain Technology	1
Figure 2.1: Blockchain vs. Book	11
Figure 3.1: Proposed model for Digital Certificate	17
Figure 5.1: Home Page	20
Figure 5.2: Student Login	21
Figure 5.3: Master data(Class/Exam Management)	22
Figure 5.4: Manage Students.....	23
Figure 5.5: Add Question & Paper.....	24
Figure 5.6: Certificate Generation(Admin side)	25
Figure 5.7: Certification Verification	26
Figure 5.8: Certificate Details.....	26
Figure 5.9: Certifiacte on Ethereum Blockchain	27

LIST OF TABLES

Table 1: Book and Block Ordering	12
---	-----------

CHAPTER 1: INTRODUCTION

1.1 GENERAL CONCEPTS

Now a day, education has become essential part of life, still we need to maintain reputation and trust in certification. Everyone has to show his/her Document and Certificate to any other person for some purpose/job. After seeing the document 3rd person cannot validate the originality of the certificate.

Blockchain - A Revolution Bigger Than the Internet

The Internet is entering the second era that's based on Blockchain [2] [3]- the Internet of Value, a new platform to change the world of business. It's novel solution to the age-old human problem of trust. It provides architecture for so-called trust less trust. It allows user to trust the outputs of the system without trusting any actor within it.

The pace with which this technology is evolving, it's making it difficult for different sectors/domains to keep, without the changes. The world is increasingly getting connected with the amalgamation of connected devices and solutions. So how do we fit in-For truly digitization process in Fintech / Banking and other sectors as well got to be seamless.

“Blockchain technology” can be seen as a group of technologies, like a bag of bricks. From the bag, we can take out bricks and put them together in different ways to create different results.

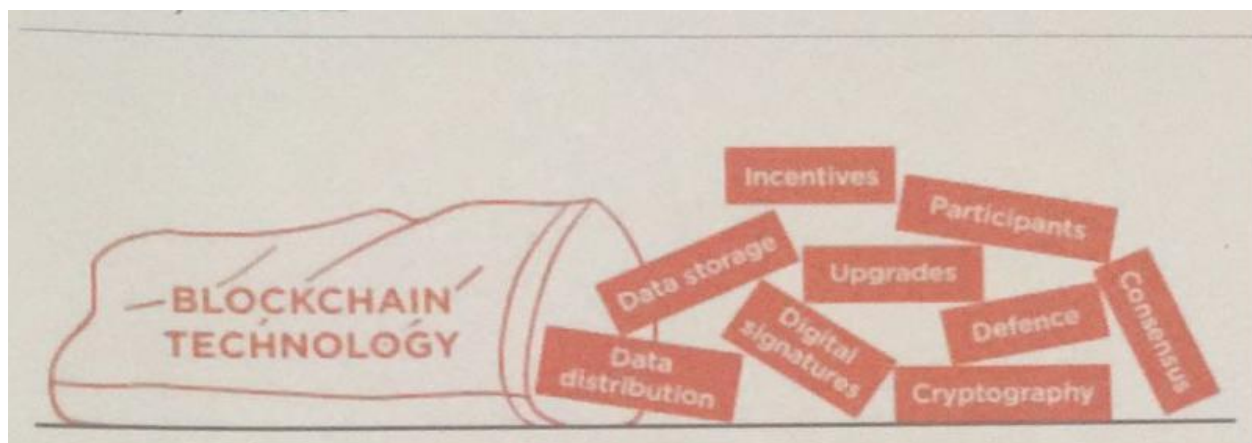


Figure 1.1: Blockchain Technology

1.2 MOTIVATION

In previous years, it has been come into the light and come in our daily routine life, that we got to know, below cases,

- Some company has fired xyz employee due to fraud educational document.
- Someone is selling the same land to the number of peoples.
- The same driving license number is issued to the number of peoples.
- Same Voter ID is issued to many peoples.
- A doctor has a fake degree, and he is doing practicing.

Many people paste the other people photograph on some other ID proof and use the scan copy/ Photocopy as an Identity proof.

From above we see that above incident happens as we have no channel to check the authenticity. If someone has a fake document, we have no options to verify the authenticity.

But when we see the cryptocurrency mechanism/ Properties, we found that it uses blockchain as a base, and it is secure by nature and has following properties.

- Decentralized
- Digital cash system
- Digital money created from code.
- Monitored by a peer to peer internet protocol.
- An encrypted string of data or a hash encoded to signify one unit of currency.

We can build the trust for education certificate by using blockchain technology. By using this technology, No need for a central authority to validate documents. Your college won't have to send you a copy of your transcript and prove to anyone you have your degree. We are building a platform that will be open, accessible and one piece of software at a time and students can get Blockchain-based educational certifications. Blockchain-based educational certifications are the digital certificate and registered on the Ethereum Blockchain that will be cryptographically signed and tamper proof

(Ethereum blockchain is on 2nd number after Bitcoin blockchain). Another person can view the certificate online, and no 3rd party validation is required for these digital certificates.

1.3 RELATED WORK

As of now, mainly Blockchain is used in cryptocurrency. When Satoshi Nakamoto (Bitcoin Developer) saw problems in centralized currency, he tried to build digital cash system without a central entity, and it will be like a Peer-to-Peer network, this became the birth of cryptocurrency.

Cryptocurrency is a method/way in the Blockchain using encryption technique to control the creation of monetary units and to verify the transfer of funds. The transaction is known instantly by the whole network. But miners take some time to confirm this transaction. This is miner's job in a cryptocurrency-network, and they get rewarded with a token (some amount) of the cryptocurrency.

In a decentralized network, we don't need a central server which keeps the record of the transaction/balances. Every node in the system has a copy of all transactions to check if current transactions are valid or not.

Top 5 Cryptocurrency (2018/03/15-as per Market Capitalization=Price* $Circulating\ Supply$)

1.3.1. Bitcoin BTC

1.3.2. Ripple XRP

1.3.3. Ethereum ETH

1.3.4. Bitcoin Cash BCH

1.3.5. Cardano ADA.

1.3.1 Bitcoin BTC:

Satoshi Nakamoto is the unknown inventor of Bitcoin. It was released in 2009, and its symbol is BTC.

"A new electronic cash system that uses a peer-to-peer network to prevent double-spending. It is completely decentralized with no central authority or server" – Satoshi Nakamoto, 09 January 2009, announcing Bitcoin on SourceForge [4]. It is a digital currency system based on peer-to-peer virtual data [5]. It uses peer-to-peer technology or network to operate with no central authority or banks; managing transactions and the issuing of Bitcoin is carried out collectively by the system.

Bitcoin is 1st cryptocurrency that usages Cryptography to control its creation and transactions, rather than a central authority. It provides a new payment system that is digital in nature and no central authority/mediators are involved. It can be considered as “Cash for Internet”.

- Market Cap: \$222,014,656,865
- Price: \$13,238.0000
- Available Supply: 16,771,012

1.3.2 Ripple XRP

Ripple was developed by Arthur Britto, David Schwartz & Ryan Fugger. It was released in 2013, and its symbol is XRP.

It is a real-time payment network that offers immediately certain and low-cost international payments. It "enables banks to settle cross-border payments in real time, with end-to-end transparency, and at lower costs." It is based around a shared, public database which uses a consensus process that allows for payments, exchanges, and remittance in a distributed process. Its Ledger does not require mining that is the major difference from Bitcoin and other cryptocurrency that uses mining concept. That's why it does not require more computing power.

- Market Cap: \$88,309,754,593
- Price: \$2.2796
- Available Supply: 38,739,144,847

1.3.3 Ethereum ETH

Ethereum was developed by the Ethereum Foundation (a Swiss non-profit foundation). It was released in 2015, and its symbol is ETH.

It is a distributed SW platform that use Smart contract to interact with the blockchain. Application based on Ethereum runs without any fraud and 3rd party validation.

- Market Cap: \$66,287,547,582
- Price: \$686.4400
- Available Supply: 96,567140

1.3.4 Bitcoin Cash BCH:

Bitcoin Cash was developed by Bitmain group. It was released in 2017, and its symbol is BCH. It is the continuation of the Bitcoin project as peer-to-peer digital cash. It is a fork of the Bitcoin blockchain ledger, with upgraded consensus rules that allow it to grow and scale. Its block size limit to eight megabytes. The rule change increasing the Bitcoin block size limit of one megabyte to eight megabytes is classified as a hard fork.

- Market Cap: \$39,092,477,988
- Price: \$2,315.4250
- Available Supply: 16,883,500

1.3.5 Cardano ADA

Cardano was developed by Aggelos Kiayias, and it was released in 2017, and its symbol is ADA.

- Market Cap: \$13,290,216,358
- Price: \$0.5126
- Available Supply: 25,927,070,538

1.4 PROBLEM STATEMENT

As education becomes more diversified, decentralized and democratized, we still need to maintain reputation, trust in certification, and proof of learning. Nowadays everyone has to show his/her Document and Certificate to any other person for some purpose/job. After seeing the document 3rd person cannot validate the originality of the certificate.

Major problem:

- Authenticity
- Trust
- Accessibility

Possible Solution:

- Database with no update feature
- Digital Signature
- Blockchain.

We are building a platform that will be open, accessible and one piece of software at a time and students can get Blockchain-based educational certifications. Blockchain-based educational certifications are the digital certificate and registered on the Ethereum Blockchain that will be cryptographically signed and tamper proof. Other people can view the certificate online, and no 3rd party validation is required for these digital certificates.

We are going to build a web-based platform for students where they can enroll and select a course, which will have two major parts,

- After choosing the course, they have to give exams and result will be saved on blockchain server.
- At admin/university/college side, they can manage courses and student profiles.

1.5 SCOPE OF THIS THESIS

Previous work in the field of the blockchain, which is mainly focused on the cryptocurrency and its mining. In 2017, the blockchain rose to a high level, Most of the attention has been on cryptocurrencies such as Bitcoin and Ethereum as investors try to catch the next wave. Now it is going to different sector- Education, Land registry, Banking Share marking....

In this Project, I have investigated the possibilities of use of blockchain technology in the education sector. I have worked on certification generation by using this technology, in which candidate will enroll for a course and have to give the online exam. After completion of the exam, if a candidate is Pass result will be saved on blockchain ledger, and if a candidate fails, the result will not be kept on blockchain and user have to reattempt the exam.

The purpose of this report/thesis is to analyze the use of new emerging technology (blockchain) in the field of education so that candidate gets the benefit and employer has the transparency. That will reduce the fraud cases as data cannot be erased/ Rewrite on blockchain server.

CHAPTER 2: LITERATURE REVIEW

2.1 BLOCKCHAIN:

Since its 2008 appearance as a cornerstone of the cryptocurrency Bitcoin, the blockchain technology gained widespread attention as a modality to securely validate and store information without a trusted third party [6]. Blockchain is a decentralized transaction and data management technology developed first for Bitcoin cryptocurrency [7]. Blockchain features a decentralized and incorruptible database that has high potential for a diverse range of uses [8].

A blockchain, originally block chain, is a continuously growing list of records, called blocks, which are linked and secured using cryptography. Each block typically contains a cryptographic hash of the previous block, a timestamp and transaction data. By design, a blockchain is inherently resistant to modification of the data. It is "an open, distributed ledger that can record transactions between two parties efficiently and in a verifiable and permanent way".

Blockchain is a decentralized ledger used to securely exchange digital currency, perform deals and transactions [8] and managed by peer to peer networks. All nodes follow same protocol for inter-node communication and validating new blocks. Once data is validated in any block it cannot be altered by any block. To alter particular block data all subsequent block data should be altered that will result in collusion of the network and that transaction will be rejected by all nodes.

In 2008, Satoshi Nakamoto invented the blockchain for the use of cryptocurrency and Bitcoin was its 1st implementation. Bitcoin was the 1st public transaction ledger. The invention of this currency solved the double-spending problem without the need of a 3rd party. After that other cryptocurrency were invented on same concept.

In short, a blockchain is a distributed database that contains a list of records (data). Distributed means that instead of being stored on a central device somewhere, the entire database is actively synced and stored on a bunch of other devices. This is called a peer-to-peer network, much like how Napster was a peer-to-peer network for sharing music files.

The main advantage this technology provides is its ability to exchange transactions without relying on trusted third party entities of any means. It can also provide data integrity, in-built authenticity and user transparency [9].

2.1.1 Blocks

A block contains set of valid transactions that are in hash form and make a Merkle Tree. Each block typically contains a hash pointer as a link to a previous block, a timestamp and transaction data. By design, blockchains are inherently resistant to modification of the data [11]. This linking forms a block of chain. This process is iterative and that confirms that previous block is reliable and correct. In this way we can go back to genesis block.

2.1.2 Block time

In blockchain block time refers to the time when network can create 1 more block in the chain. It time vary from blockchain to blockchain some blockchain allows new block as frequently as every five seconds. This time also include the time in which data becomes verifiable. In cryptocurrency term shorter block time means faster transaction. In Ethereum Blockchain Block time is approximate 14~15 seconds, while for Bitcoin is approx 10 minutes.

2.1.3 Decentralization

Blocks are stored in different locations (nodes) so blockchain eliminates a number of risks which comes if data is in single location/storage. In which we don't have no central point of failure. . Data stored on the blockchain is generally considered incorruptible, while centralized data is more easily controlled, information and data manipulation are possible.

2.2 BLCOKCHAIN WORKING:

Blockchain can be considered as the "Internet of value". On the Internet, anyone can write data and others can read it. In terms of cryptocurrency Keys fills the role of recording the transfer, which is traditionally carried out by banks. It also fills a second role, establishing trust and identity, because no one can edit a blockchain. The major functions carried out by banks - verifying identities to prevent fraud and then recording legitimate transactions -can be carried out by a blockchain more quickly and accurately.

Block orders in a blockchain

Blockchain can be considered as a book where, Blocks in a chain = pages in a book

A book has number of pages and each page contains:

- **The text:** the information/data.
- **Information about itself:** Chapter number, Title or Page number which tells where we are in the book

Similarly, in a blockchain block, each block has:

- **The contents** of the block, for example in Bitcoin are it the Bitcoin transactions and the miner incentive reward.
- **Headers** which contain the data about the block. It includes some technical information about the block, a reference to the previous block, and a fingerprint (hash) of the data contained in this block.

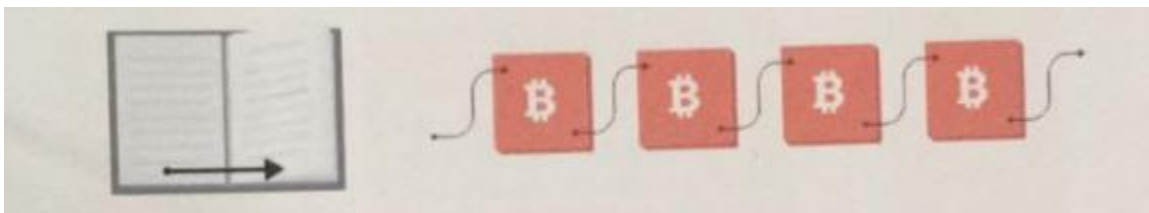


Figure 2.1: Blockchain vs. Book

Page by page: In book, Pages have page number in order. If some pages are missed and shuffled then it easy to put them back into correct order so that information can be provided in proper way.

Block by block: In Blockchain, each block have previous block address and previous block have its previous block address till genesis block.

BOOK ORDERING	BLOCK ORDERING
Page 1,2,3,4,5	Block n58ufO built on 84n855 , Block 90fk5n built on n58ufO, Block 8n6d71 built on 90fk5n.
Implicit that the page builds on the page whose number is one less. eg Page 5 builds on page 4 (5 minus 1)	84n855 ,n58ufO, 90fk5n,8n6d71 represent fingerprints or hashes of the blocks.

Table 2.1: Book and Block Ordering

2.3 PUBLIC AND PRIVATE BLOCKCHAIN:

Blockchains can be divided into 2 major categories (Public and Private). Another way of describing public/private might be Permissionless vs. Permissioned or pseudonymous vs. identified participants.

2.3.1 Public Blockchains

It has below 2 basic properties:

- Anyone, without permission granted by another authority, can write data
- Anyone, without permission granted by another authority, can read data

1st blockchain, Bitcoin is designed as a 'anyone-can-write' blockchain, where participants can add to the ledger without needing approval (**there is no 'boss' to decide**). Some of the largest, most known public blockchains are Bitcoin and Ethereum.

2.3.2 Private Blockchain

Private Blockchain provides a network where participants are known and trusted in which many rules/protocol aren't needed (or rather they are replaced with legal contracts) as participants will behave properly because he has signed this piece of paper. They do not rely on anonymous nodes to validate transactions.

2.4 CRYPTOCURRENCY:

Cryptocurrency is a medium of created, stored and exchanged electronically in the Blockchain using encryption technique to control the creation on monetary units and to verify the transfer of funds.

The transaction is known instantly by the whole network. But minors take some time to confirm this transaction. This is minor's job in a cryptocurrency-network, and in return they gets cryptocurrency token.

In a decentralized network, we don't need a central server who keeps record about the transactions. Every peer in the network needs to have a list of all transactions to check if current transactions are valid or an attempt to double spend.

2.4.1 Cryptocurrency Mining

Because of the random nature of hashing, achieving an acceptable block is never a guarantee. Thus, Bitcoin mining is a competitive venture, where miners are awarded new Bitcoin for each block successfully hashed and accepted in the blockchain [5].

Bitcoin mining is a process of creating new Bitcoin by verifying the transactions in the Bitcoin network. Every transaction is kept in a public ledger, and that ledger is verified and maintained by all of the computers participating in the Bitcoin network. This "chain" of transactions is known as the blockchain, and each transaction is essentially a public timestamp that can contain data [12].

Bitcoin miners donate their computer's processing power to run complex calculations. Who resolves the problem gets new cryptocurrency token as fees.

Miners, a decentralized network of users, validate and confirm transactions and they have setup of dedicated hardware to perform calculations, called 'hashes'. They vote with their CPU power, expressing their acceptance of valid blocks by working on extending them and rejecting invalid blocks by refusing to work on them [4]. These strings of records (hashes) that keep track of every Bitcoin transaction and replicated on every system in the Bitcoin network.

The electricity power used to "mine" the cryptocurrency is a crucial factor as its prices are skyrocketing. According to the Bitcoin analysis blog Digiconomist, people mining the cryptocurrency across the globe are using more than 30 terawatts-hours of energy. This is higher than the individual energy usage of at least 159 countries like Hungary, Oman, Ireland, and Lebanon [11].

Ethereum is the world's second-largest Blockchain network after Bitcoin and uses one-third the energy of Bitcoin. Approx 11 terawatt-hours a year, Ethereum use electricity which is the electricity consumption of Zambia. As Cryptocurrency mining is increasingly popular, its algorithm gets more and more difficult over time.

“More energy efficient algorithms, like proof-of-stake, have been in development over recent years. Bitcoin and mostly other cryptocurrency use proof-of-work methodology that required more energy consumption as compare to proof-of-stake algorithms. For Bitcoin mining operation setup, you need a place where energy costs are low. That's why an estimated 58 percent of global Bitcoin mining takes place in china.

CHAPTER3: PROPOSED WORK

3.1 DIGITAL CERTIFICATE GENERATION:

If students have an option to give exam on web base portal, after completion of exam, results/Certificate is saved on Blockchain. In this case other person can view the certificate online and no 3rd party validation is required for these digital certificates.

We are proposing a web base portal for university/college/institution and students that will provide option to student to get certificate on blockchain and minimize the option of fraud and duplicate education certificate.

Blockchain-based educational certifications are registered on the Ethereum Blockchain that will be secure and tamper proof as data cannot be erased/ Rewrite on blockchain server. Since a blockchain is a permanent record of transactions that are distributed, every transaction can irrefutably be traced back to exactly when and where it happened. In addition, past transaction cannot be changed, while the present can't be hacked, because every transaction is verified by every single node in the network.

In this web-based portal, student and admin (university/Institution) will have login access and other than student and admin can view exam details and verify certificate. It will have below two major parts,

- Student can select course, give exams and after successful completion can get certificate on blockchain.
- Admin can manage student, courses papers and question bank and can generate certificate on blockchain.

3.2 PROPOSED MODEL:

In below figure, proposed model is shown.

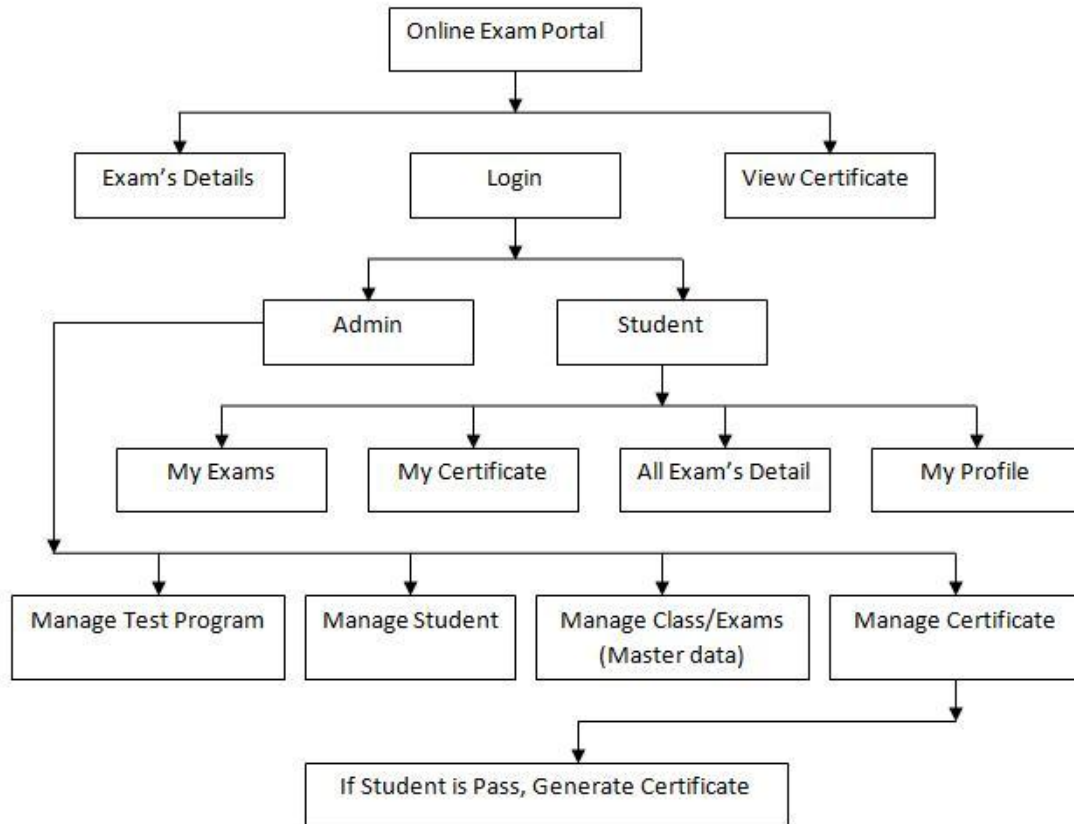


Figure 3.1: Proposed model for Digital Certificate

CHAPTER4. METHODOLOGY

We will use Ethereum blockchain to save student data/certificate. For that we need write Smart Contract that is an interface to connect on blockchain.

4.1 SMART CONTRACTS:

Solidity is a language used for smart contracts on the Ethereum blockchain [14] and it is a set of code and data that have permanent address on the Ethereum blockchain. In Object Oriented Programming language, it is similar to class where it includes state variables & functions. Smart Contracts and blockchain are the basis of all Decentralized Applications. Contracts and blockchain have immutable and distributed feature as common feature. If they are on blockchain then it will be painful to upgrades contracts.

Our contract will include:

4.1.1 State Variables-variables that hold values that are permanently stored on the Blockchain. We will use state variables to hold Student name, Course detail, Certificate number and validity date.

4.1.2 Functions-Functions are the executables of smart contracts. They are what we will call to interact with the Blockchain, and they have different levels of visibility, internally and externally. Keep in mind that whenever you want to change the value/state of a variable, a transaction must occur-costing Ether.

4.1.3 Events-Whenever an event is called, the value passed into the event will be logged in the transaction's log. This allows JavaScript callback functions or resolved promises to view the certain value you wanted to pass back after a transaction. This is because every time you make a transaction, a transaction log will be returned. We will use an event to log the ID of the newly created Candidate, which we'll display.

4.2 THE ETHERIUM VIRTUAL MACHINE (EVM) :

Ethereum Virtual Machines is implemented in C++, Go, Haskell, Java, JavaScript, and Python. It is the runtime environment for smart contracts in Ethereum. It handles the internal state and computation of the entire Ethereum Network.

4.3 GAS:

Gas is the internal pricing that we have to pay for running a transaction or contract in Ethereum blockchain. A certain number of gas occurred whenever there is an operation performed by transaction or contract on the Ethereum platform.

Any computer code (complex or short) can be run inside EVM, A short code can result in more computation work as compare to complex code. It means that short code ode not guarantee less computation work. Gas depends upon the calculation done inside the EVM; our focus should be on less computation work that will result in less amount of Gas. Its payment is charged as a certain number of ether. The transaction fee is Transaction fee is combination of total gas used multiplied by gas price.

We will also use below tools:

Web3.js is a JavaScript API and with the help of this API We can interact with the Blockchain - making transactions and calls to smart contracts. Developer can focus on the content of their application as this API abstracts the communication with Ethereum Clients.

Truffle is a testing development framework for Ethereum. It includes a development blockchain, compilation and migration scripts to deploy your contract to the Blockchain, contract testing, and so on. It makes development easier.

CHAPTER5: EXPERIMENTAND RESULTS

5.1. TOOLS USED:

We will run our portal in Web browser, Student and Admin (College/University) both have access for Login. On Home Page Login, Exams details and View Certificate will be available.

No Login will be required for details and View Certificate; anyone can view Certificate by entering Certificate number.

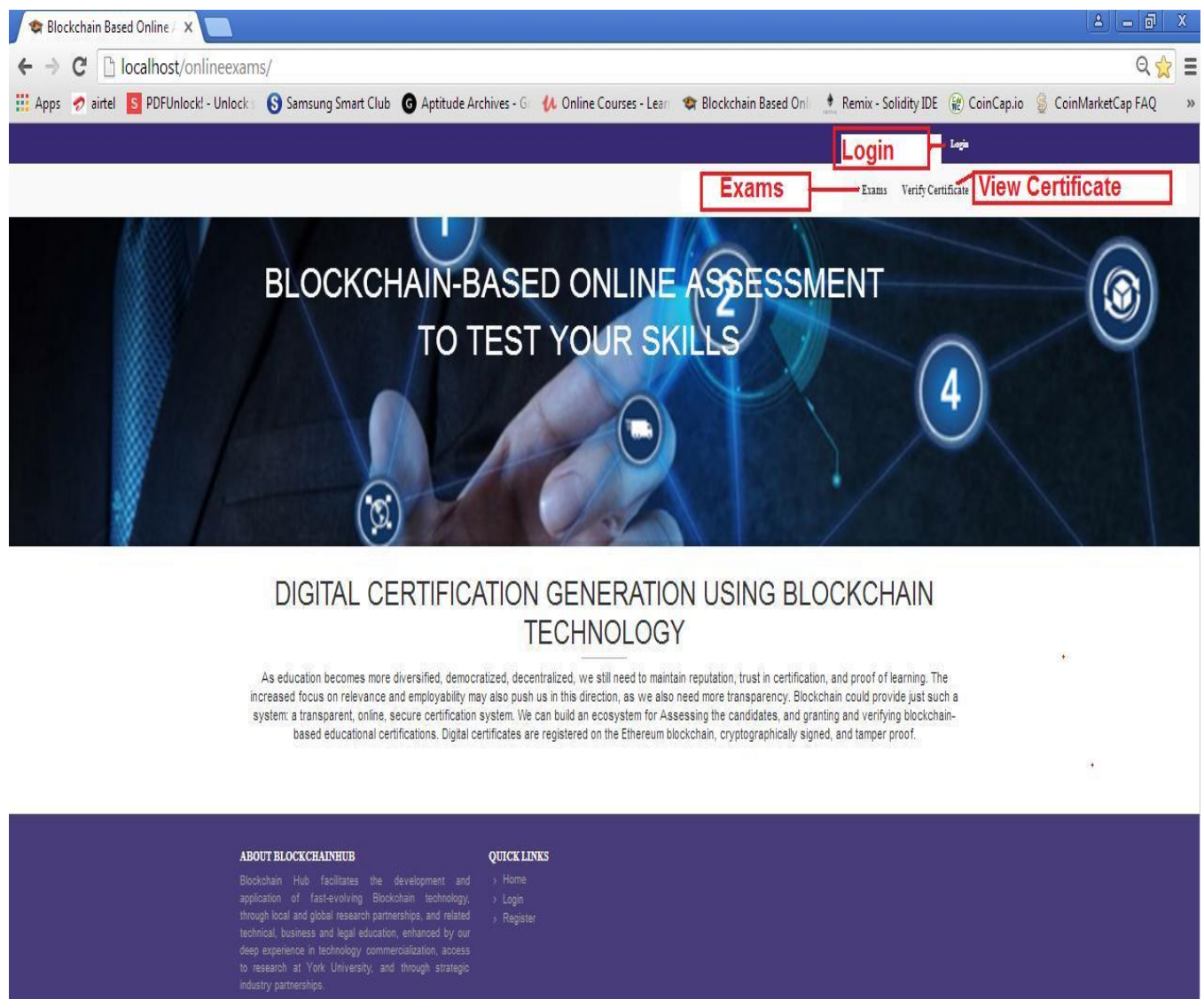


Figure 5.1: Home Page

Student Login

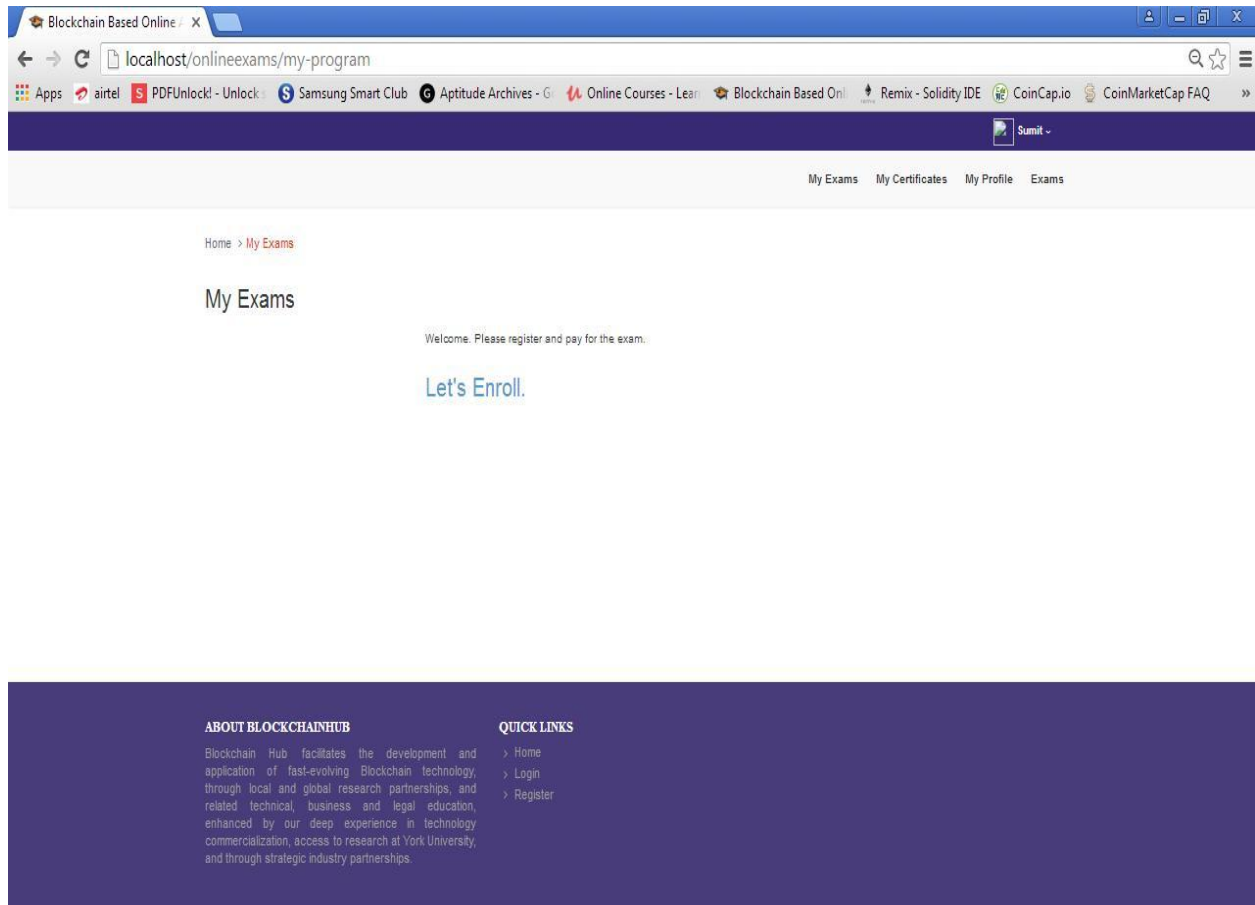


Figure 5.2: Student Login

From Admin side, We can add Courses,Subject,Units , Chapters and Topic.We can see the same thing in below Image . S1U1C1T1 represents Subject 1->Unit1->Chapter1->Topic1.

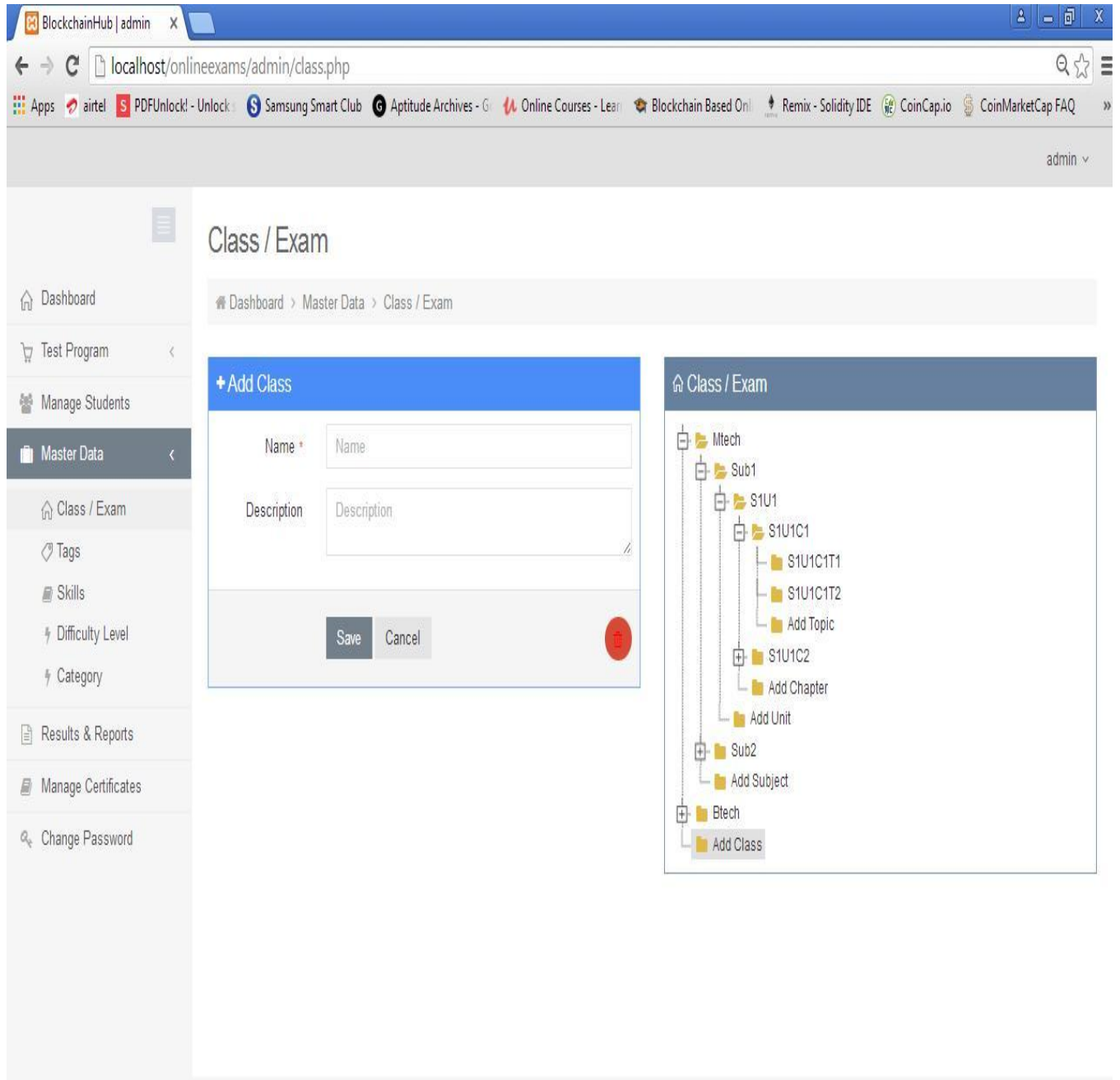
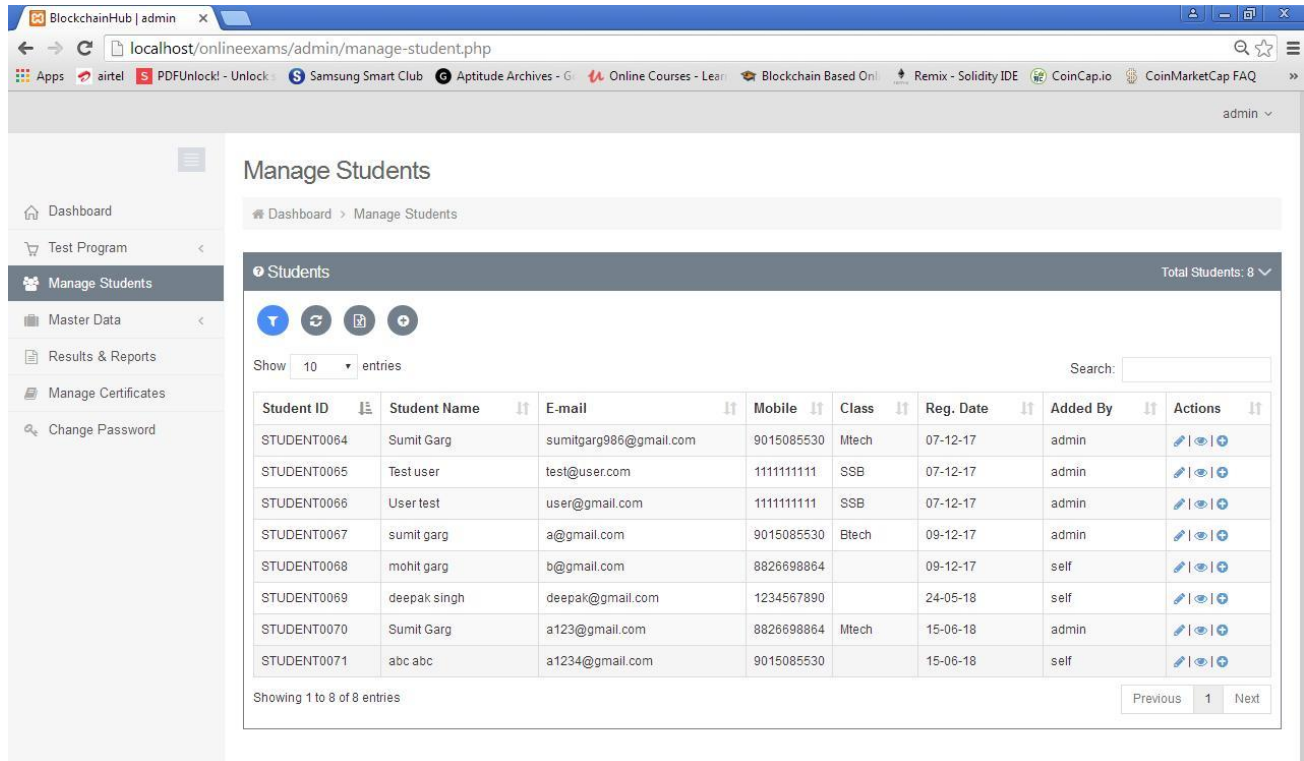


Figure 5.3: Master data(Class/Exam Management)

We can manage student data from admin side adding deleting and modification to student details.

Student data contains Student Name,Email ID Mobile Number and Class. By default login password will be Student Mobile number.



The screenshot shows a web browser window with the URL `localhost/onlineexams/admin/manage-student.php`. The page title is "Manage Students" and the breadcrumb is "Dashboard > Manage Students". The interface includes a sidebar with navigation options: Dashboard, Test Program, Manage Students (selected), Master Data, Results & Reports, Manage Certificates, and Change Password. The main content area displays a table of students with the following data:

Student ID	Student Name	E-mail	Mobile	Class	Reg. Date	Added By	Actions
STUDENT0064	Sumit Garg	sumitgarg986@gmail.com	9015085530	Mtech	07-12-17	admin	✎ 👁 🗑
STUDENT0065	Test user	test@user.com	1111111111	SSB	07-12-17	admin	✎ 👁 🗑
STUDENT0066	User test	user@gmail.com	1111111111	SSB	07-12-17	admin	✎ 👁 🗑
STUDENT0067	sumit garg	a@gmail.com	9015085530	Btech	09-12-17	admin	✎ 👁 🗑
STUDENT0068	mohit garg	b@gmail.com	8826698864		09-12-17	self	✎ 👁 🗑
STUDENT0069	deepak singh	deepak@gmail.com	1234567890		24-05-18	self	✎ 👁 🗑
STUDENT0070	Sumit Garg	a123@gmail.com	8826698864	Mtech	15-06-18	admin	✎ 👁 🗑
STUDENT0071	abc abc	a1234@gmail.com	9015085530		15-06-18	self	✎ 👁 🗑

Showing 1 to 8 of 8 entries. Search:

Figure 5.4: Manage Student

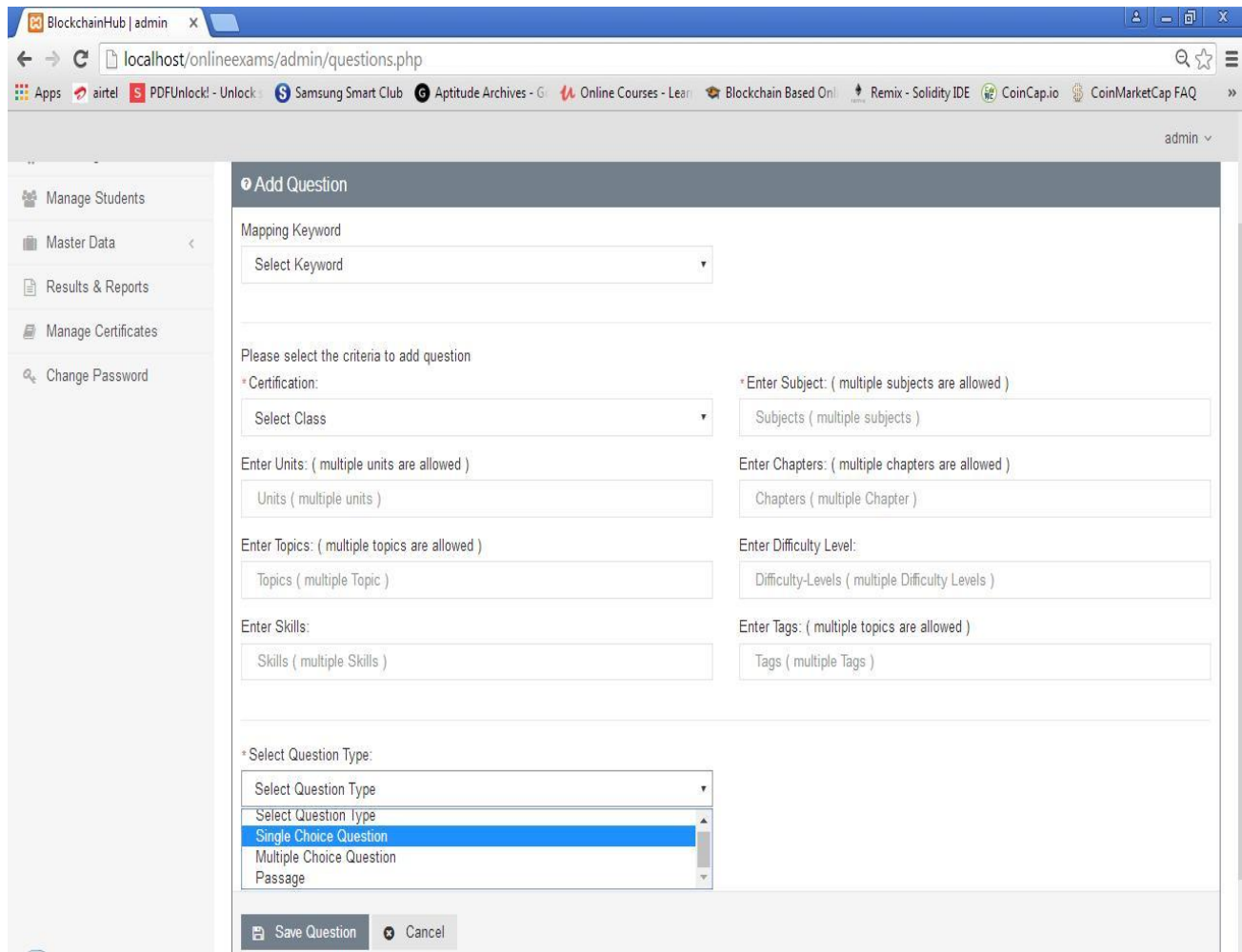


Figure 5.5: Add Question & Paper

5.2 Results: Once Students Clears the Exam Generate Option will be available at Admin Side,After clicking on Generate options Contract will be called and Student data will be sent to Blockchain That will contains Student name, Course detail, Certificate number and validity date.

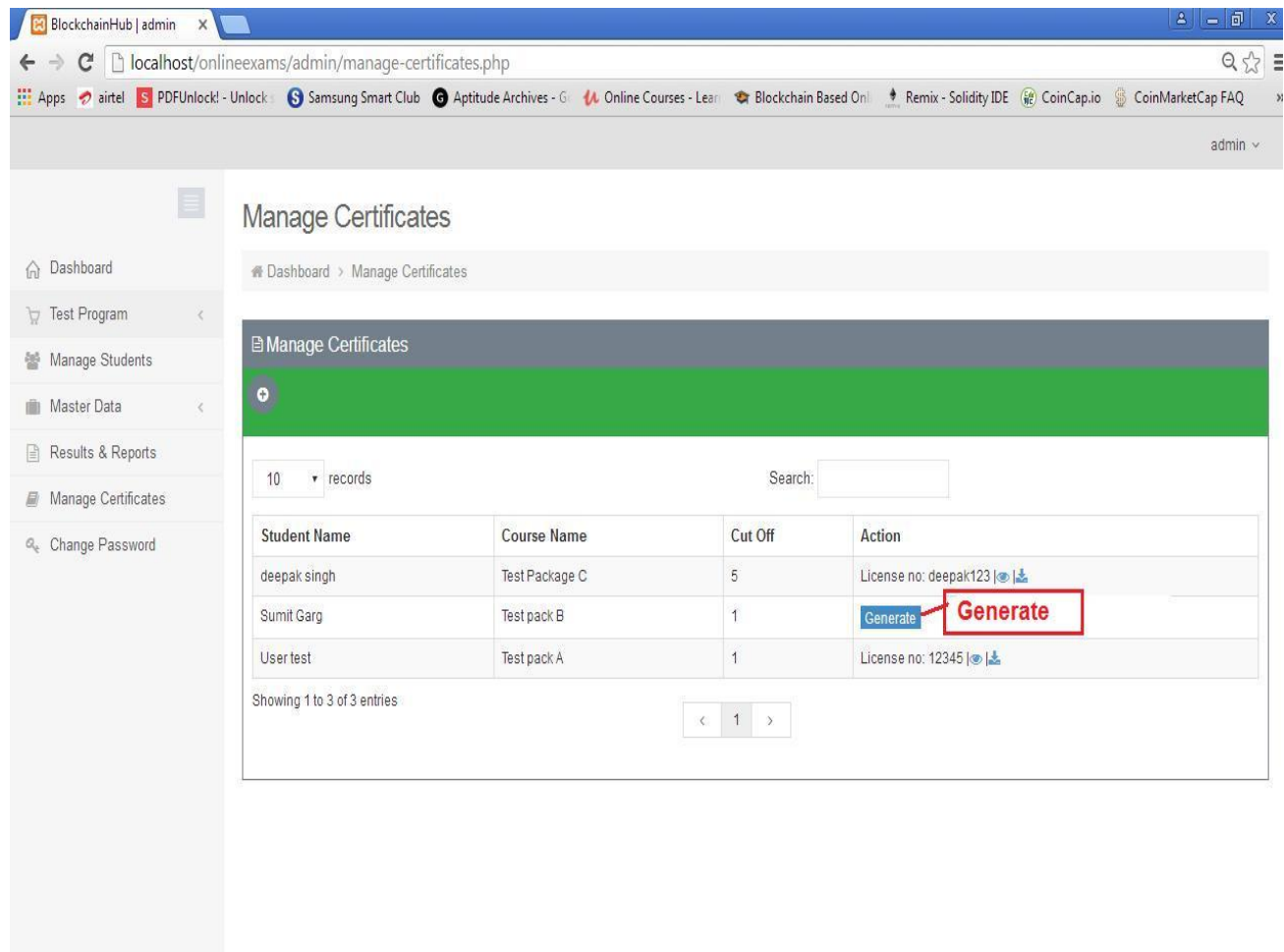


Figure 5.6: Certificate Generation(Admin side)

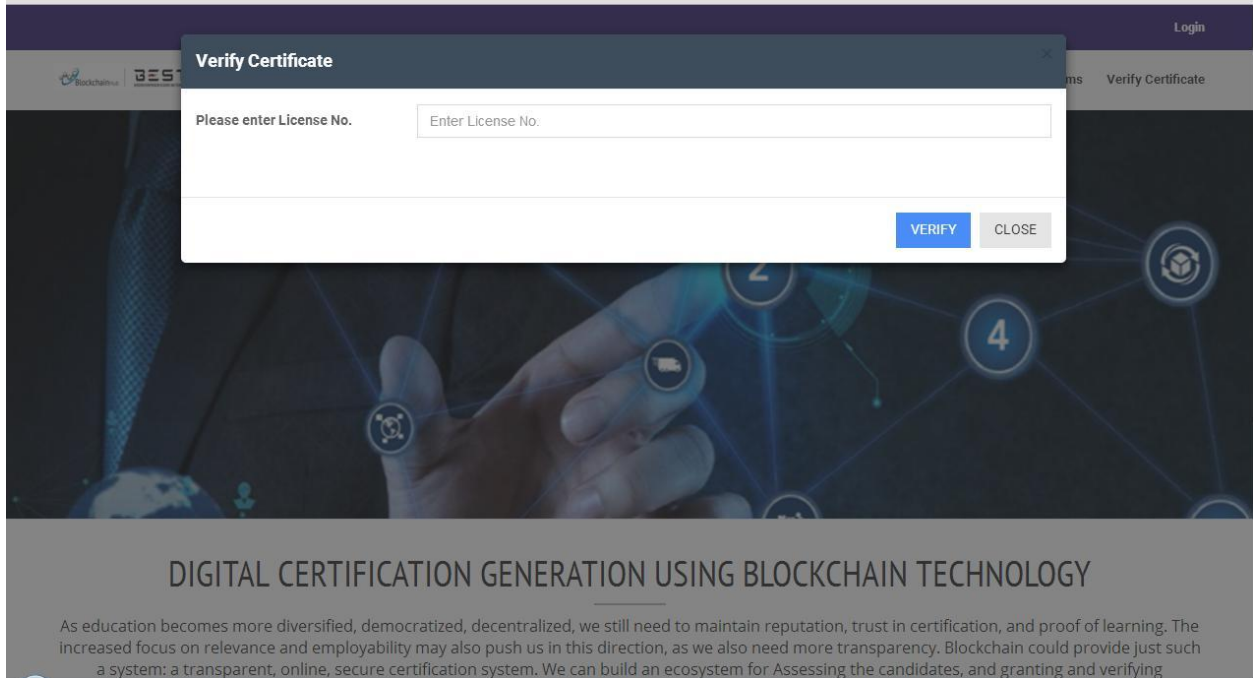


Figure 5.7: Certification Verification

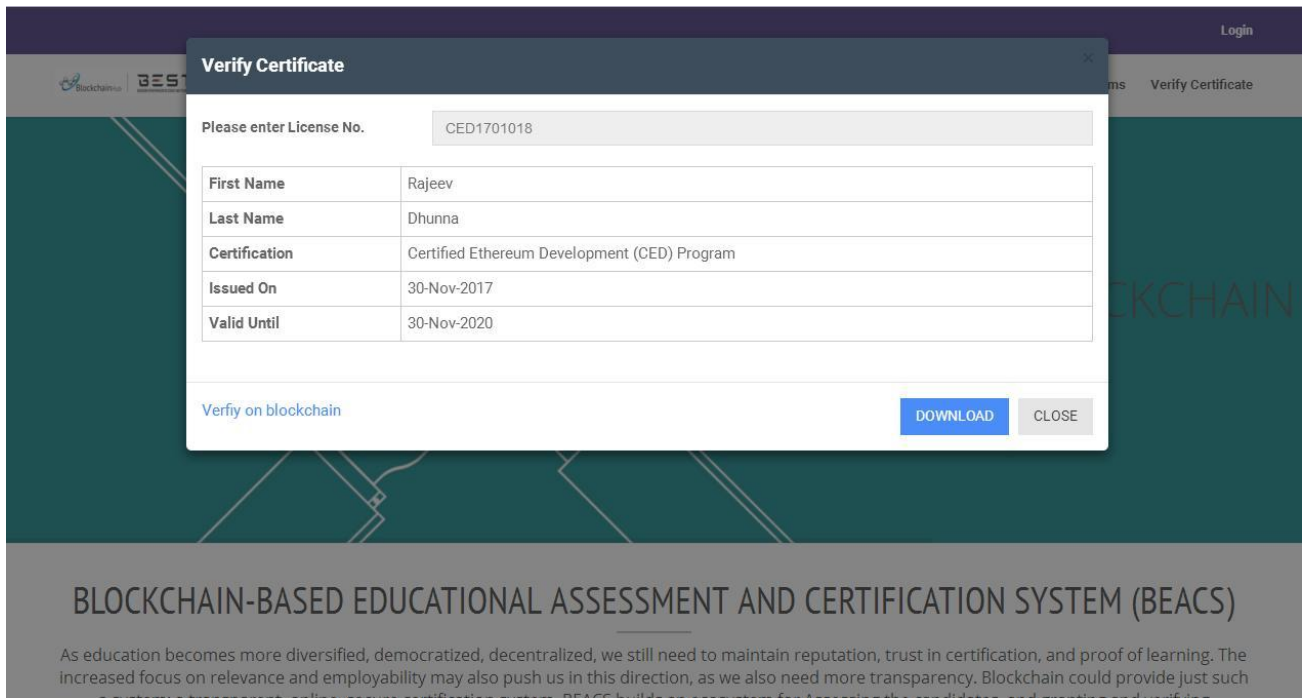


Figure 5.8: Certificate Details

CHAPTER 6: CONCLUSION

As of now we are using internet (which is decentralized online platform) to sharing information. But when we transfer money; we are using old-fashioned, centralized financial establishments like banks. In other areas we are also using centralized system to share information (like education- where university has full control).

Blockchain technology provides a way to eliminate this "middleman/central authority. It does this by filling three important roles – recording transactions, establishing identity and establishing contracts. Information security is one of the most important features of Blockchain [6].

Blockchain can be used to store any type of digital information (e.g. computer code) rather than cryptocurrency usages .Previous work in the field of the blockchain, which is mainly focused on the cryptocurrency and it's mining. In 2017, the blockchain rose to a high level, Most of the attention has been on cryptocurrencies such as Bitcoin and Ethereum as investors try to catch the next wave. Now it is going to different sector-Education, Land registry, Banking Share marking....

For truly digitization process in Banking and other sectors, we can use Blockchain technology as a base. It will build trust and provide a way that someone can verify the other person documents in less time and validate the originality.

If we use blockchain in Education/Land Registry/ID card verification/Banking sector, then it will be a **“1st step towards corruption free country.”**

REFERENCES

- [1] Lyndon Lyons and Andreas Bachmann Jan Seffinga, "The Blockchain (R)evolution –The Swiss Perspective," , Switzerland, 2017.
- [2] Don Tapscott and Alex Tapscott, "Realizing the Potential of Blockchain-A Multistakeholder Approach to the Stewardship of Blockchain and Cryptocurrencies," in *World Economic Forum*, 2017.
- [3] Alex Tapscott, BLOCKCHAIN REVOLUTION:Understanding the 2nd Generation of The Internet and the New Economy, 2017.
- [4] Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, 2008, White Paper.
- [5] George F. Hurlburt and Irena Bojanova, "Bitcoin: Benefit or Curse?," in *IEEE*, 2014.
- [6] Nicola Dimitri, The Blockchain Technology: Some Theory and Applications, 2017, MSM-Working Paper No. 2017/03.
- [7] Deokyoon Ko, Sujin Choi, Sooyong Park, Kari Smolander Jesse Yli-Huumo, "Where Is Current Research on Blockchain Technology?—A Systematic Review," October 2016.
- [8] Nirmala Singh and Sachchidanand Singh, "Blockchain: Future of financial and cyber security," in *IEEE*, Noida, 2016.
- [9] Engin Zeydan and Suayb Sb Arslan Gültekin Berahan Mermer, "An overview of blockchain technologies: Principles, opportunities and challenges," in *IEEE*, Turkey, 2018.
- [10] Narn-Yih Lee , Chien Chi and Yi-Hua Chen Jiin-Chiou Cheng, "Blockchain and smart contract for digital certificate," in *IEEE*, Japan, 2018.
- [11] Henrique Rocha ,Marcus Denker and Stephane Ducasse Santiago Bragagnolo, "SmartInspect: solidity smart contract inspector," in *IEEE*, Itly, p. 2018.
- [12] GWYN D'MELLO. (2017, Dec.) <https://www.indiatimes.com/technology/news>. [Online].
<https://www.indiatimes.com/technology/news/bitcoin-miners-are-using-more-electricity-than-ireland-other-159-countries-no-kidding-335114.html>

[13] Abdul Wadud Chowdhury. (2017, Nov.) <https://medium.com>. [Online].

<https://medium.com/oceanize-geeks/blockchain-and-the-future-of-digital-trust-354acc279acc>

[14] Nick Grossman. (2015, June) <https://www.nickgrossman.is>. [Online].

<https://www.nickgrossman.is/2015/the-blockchain-as-time/>