

MARKSHEET VERIFICATION USING BLOCKCHAIN

Submitted in partial fulfilment of the requirements for the award of Bachelor of Engineering degree in Computer Science and Engineering

by

A Vikranth (Reg.No.37110057)
A Sujith Kumar(Reg.No.37110038)



DEPARTMENT OF COMPUTER SCIENCE AND
ENGINEERING SCHOOL OF COMPUTING

SATHYABAMA

INSTITUTE OF SCIENCE AND TECHNOLOGY
(DEEMED TO BE UNIVERSITY)

Accredited with Grade "A" by NAAC | 12B Status by UGC | Approved
by AICTE

JEPPIAAR NAGAR, RAJIV GANDHI SALAI, CHENNAI – 600 119

MARCH - 2021



SATHYABAMA

INSTITUTE OF SCIENCE AND TECHNOLOGY

(DEEMED TO BE UNIVERSITY)

Accredited with "A" grade by NAAC I 12B Status by

UGC I Approved by AICTE

Jeppiaar Nagar, Rajiv Gandhi Salai, Chennai - 600119

www.sathyabama.ac.in



DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

BONAFIDE CERTIFICATE

This is to certify that this Project Report is the bonafide work of **A Vikranth (37110057)** and **A Sujith Kumar (37110038)** who carried out the project entitled **Marksheet Verification using Blockchain** under my supervision from November 2020 to March 2021.

Internal Guide

Dr. Ulagamuthalvi, M.E., Ph.d.,

Head of the Department

Submitted for Viva voce Examination held on _____

Internal Examiner

External Examiner

DECLARATION

I **A SUJITH KUMAR** hereby declare that the Project Report entitled **MARKSHEET VERIFICATION USING BLOCKCHAIN** is done by me under the guidance of **Dr. Ulagamuthalvi, M.E., Ph.d.**, Department of Computer Science and Engineering at Sathyabama Institute of Science and Technology is submitted in partial fulfillment of the requirements for the award of Bachelor of Engineering degree in Computer Science and Engineering.

DATE:

PLACE: CHENNAI

SIGNATURE OF THE CANDIDATE

ACKNOWLEDGEMENT

I am pleased to acknowledge my sincere thanks to **Board of Management of SATHYABAMA INSTITUTE OF SCIENCE AND TECHNOLOGY** for their kind encouragement in doing this project and for completing it successfully. I am grateful to them.

I convey my thanks to **Dr. T. Sasikala, M.E., Ph.D., Dean**, School of Computing, **Dr. S. Vigneswari, M.E., Ph.D., and Dr. L. Lakshmanan, M.E., Ph.D., Heads of the Department** of Computer Science and Engineering for providing me necessary support and details at the right time during the progressive reviews.

I would like to express my sincere and deep sense of gratitude to my Project Guide **Dr. Ulagamuthalvi, M.E., Ph.d.**, for her valuable guidance, suggestions and constant encouragement paved way for the successful completion of my project work.

I wish to express my thanks to all Teaching and Non-teaching staff members of the **Department of Computer Science and Engineering** who were helpful in many ways for the completion of the project.

ABSTRACT

The blockchain is an incorruptible digital ledger of economic transactions that can be programmed to record not just financial transactions but virtually anything of value. Blockchain techniques maintain transparency of data on all its peers on the network. This technique can be applied in various fields. The blockchain technique is considered to be very secure in terms of protecting data. Each block in a blockchain consists of a hash value of the previous block and a ledger that is stored redundantly across many nodes. Once the data is recorded in the blockchain it becomes difficult to change that data. In the present system of marksheet verification in order to check the originality of marksheet the company needs to contact the concerned institution/university to validate the marksheet. In this regard a lot of time and human resources are wasted to accomplish this process. In the proposed system using blockchain, we are making marksheet verification easier and secure so that nobody can temper with the marksheet once the mark sheet is stored on the blockchain. Also, the marksheet can be verified by comparing the hash value to the one stored in the blockchain.

TABLE OF CONTENTS

CHAPTER NO.	TITLE	PAGE NO.
	ABSTRACT	v
	LIST OF FIGURES	viii
1	INTRODUCTION	1
	1.1 Introduction	1
	1.2 Blockchain	2
	1.3 Advantages of Blockchain	3
2	AIM AND SCOPE	5
	2.1 Aim of Project	5
	2.1.1 Objectives	5
	2.2 Scope	5
	2.3 Literature Review	6
3	SYSTEM DESIGN & METHODOLOGY	8
	3.1 Existing System	8
	3.2 Proposed Work	8
	3.3 System Design	9
	3.4 Process	10
4	SOFTWARE DEVELOPMENT METHODOLOGY	11
	4.1 Requirement Specification	11
	4.1.1 Hardware Requirements	11
	4.1.2 Software Requirements	11
	4.2 Blockchain	12
	4.3 Features of Blockchain	12
	4.3.1 Increased Capacity	13
	4.3.2 Better Security	13
	4.3.3 Immutability	13

	Faster Settlement	13
	Decentralized System	13
	Minting	14
	Hyperledger	14
	Membership Service Provider	14
	Certification Authority	14
	Business Network	15
	Fabric Composer	15
	Smart Contracts and Chaincode	15
	Nodejs	16
	Features of Nodejs	16
	Fabric-Contract-API	17
	Fabric-Shim	17
	Go Programming	17
5	RESULTS AND DISCUSSION	19
	Creating Student	19
	Get Student	20
	Issue Certificate	20
	Verify Certificate	21
6	CONCLUSION AND FUTUREWORK	22
	Conclusion	22
	Future Work	22
	REFERENCES	23
	APPENDIX	25
	A)Plagiarism Report	25
	B)Journal Paper	26
	C)Source Code	30

LIST OF FIGURES

FIGURE NO.	FIGURE NAME	PAGE NO.
3.1	System Design	9
4.1	Features of Blockchain	12
5.1	Creating Student	19
5.2	Get Student	20
5.3	Issue Certificate	20
5.4	Verify Certificate	21

CHAPTER 1

INTRODUCTION

N

INTRODUCTION

Universities issue certificates to students who have completed the graduation. A graduation certificate is mostly in the form of a paper-based document, an electronic document cannot effectively replace a physical certificate. However, due to the presence of advanced and cheap scanning and printing technologies, the forgery of certificates has increased. This threatens the integrity of the certificate holder and the university that issued the certificate.

It is necessary to validate that the graduation certificate presented by the graduate is genuine and the holder is the rightful owner. Moreover, a graduation certificate has to be verified to ensure that its content is correct and also to ensure that the certificate comes from an authentic source. To check the validity, much time will be spent in either reaching out to the university to verify a certificate or in awaiting a reply from the university to confirm that the certificate is valid, and the information is accurate. This process can be extremely laborious and expensive. Making certificates easily verifiable is one advantage of digital systems. In our project, we have decided to explore the field of Blockchain to implement our solution. The platform used for implementation is Hyperledger.

The Blockchain concept was proposed as bitcoin by Satoshi Nakamoto in early 2008. Blockchain is a distributed ledger which provides decentralized and data sharing. Each Block contains set of transaction, these transactions could be cryptocurrency transaction, digital certificate, bill of lading etc., the transaction data should replicate to all the nodes to form identical transaction details in ledger. The transaction details are validated by intermediators, there after the valid transactions are updated and new mined block will be appended with longest chain. Blockchain

transaction are cryptographically sealed which ensure security Verification of mark sheets is a tedious process for the industries to carry out, which often contact the respective

university/college to cross verify the mark sheets of individuals who have passed out from that particular university or college.

Counterfeit certificates is an issue, as any particular industry needs time to authenticate if the certificates of any student are genuine. In the block chain there is no centralized ledger but we use a decentralized ledger that means the same data is present with the members of that block chain. This data is always kept updated with its transaction. First the mark sheets of students will be created. The HOD will authenticate the digital certificate and will mark it with digital signature and it will be given to student and its cryptographic hash will be stored on the Blockchain. The student's digital certificate can be verified for authenticity by anyone who has the DAPP for our project.

The DAPP will convert the digital certificate to its cryptographic hash and check if it matches the copy in the block to prove authenticity. Graduation certificates and mark sheets contain information confidential to the individuals and should not be easily accessible to others. Hence, there is a high need for a mechanism that can guarantee that the information in such a document is original, which means that the document has originated from an authorized source and is not fake. Verification of mark sheets is a tedious process for the industries to carry out, which often involves contacting the respective universities/colleges to cross verify the mark sheets. Any particular industry needs time to authenticate if the certificates of any student are genuine.

BLOCKCHAIN

A Blockchain is essentially a distributed database of records or public ledger of all transactions or digital events that have been executed and shared among participating parties. Each transaction in the public ledger is verified by consensus of a majority of the participants in the system. And, once entered, information can never be erased. The Blockchain contains a certain and verifiable record of every single transaction ever made. To use a basic analogy, it is easy to steal a cookie from a cookie jar, kept in a secluded place than stealing the cookie from a cookie jar kept in a market place, being observed by thousands of people. Bitcoin is the most popular

example that is intrinsically tied to Blockchain technology. It is also the most controversial one since it helps to enable a multibillion-dollar global market of anonymous transactions without

any governmental control. Hence it has to deal with a number of regulatory issues involving national governments and financial institutions. However, Blockchain technology itself is non-controversial and has worked flawlessly over the years and is being successfully applied to both financial and non-financial world applications. Last year, Marc Andreessen, the doyen of Silicon Valley's capitalists, listed the Blockchain distributed consensus model as the most important invention since the Internet itself. Johann Polychaeta from BNP Paribas wrote in the Quintessence magazine that bitcoin's blockchain, the software that allows the digital currency to function should be considered as an invention like the steam or combustion engine that has the potential to transform the world of finance and beyond.

Current digital economy is based on the reliance on a certain trusted authority. Our all online transactions rely on trusting someone to tell us the truth—it can be an email service provider telling us that our email has been delivered; it can be a certification authority telling us that a certain digital certificate is trustworthy; or it can be a social network such as Facebook telling us that our posts regarding our life events have been shared only with our friends or it can be a bank telling us that our money has been delivered reliably to our dear ones in a remote country. The fact is that we live our life precariously in the digital world by relying on a third entity for the security and privacy of our digital assets. The fact remains that these third-party sources can be hacked, manipulated or compromised. This is where the blockchain technology comes handy. It has the potential to revolutionize the digital world by enabling a distributed consensus where each and every online transaction, past and present, involving digital assets can be verified at any time in the future. It does this without compromising the privacy of the digital assets and parties involved. The distributed consensus and anonymity are two important characteristics of blockchain technology.

ADVANTAGES OF BLOCKCHAIN

In the Blockchain, there is no centralized ledger but we use a decentralized ledger that means the same data is present with the members of that Blockchain. This data is always kept updated with its transaction. First, the mark sheets of students will be created. The higher authorities will authenticate the digital certificate and will mark it

with a digital signature and it will be given to the student and its cryptographic hash will be stored on the Hyperledger Blockchain. We are going to produce the

decentralized certificate verification application on the Blockchain. We choose this technology because it is traceable, tamper-proof, and encrypted. By integrating the Blockchain technology we will be able to eradicate the problem of fake certificates. We will use a smart contract at the backend to interact with the Blockchain and the encrypted hash value of each document will be stored in the Blockchain which will be verified against the user document.

Before Blockchain was used in crypto currency, particularly in the domain of cryptography and data structure. The hash tree was the primitive form of Blockchain, also known as Merkle Tree. This data structure functioned by verifying and handling data between computer systems. The validation of data was important to make sure nothing was changed or altered and also ensure that false data was not sent during transmission in a peer-to-peer network of computers. It is used to maintain and prove the integrity of data being shared.

Blockchain would contain a secure history of data exchanges and utilize peer to peer network to timestamp and verify its exchange. Blockchain is a decentralized database that records the data, like finance contracts, physical assets and supply chain information. It has acquired a successful recognition over time and used by Bitcoin. The two phrases of Blockchain are: Block and Chain. Block is the original entity that documents the time stamp and is encrypted. By use of a private key it is governed by an owner.

All the distributed chains are updated on the real-time basis in case of edits introduced. It is the most active part of the Blockchain that records the previous transactions. On completion, the block moves back to the Blockchain and the new one is generated which forms the chains that are linked to one another. The new developed block gets connected to the previous block. The complete history of the users and addresses are contained in the Blockchain. The copy of the data cannot be regenerated while distribution of data. While making a transaction, anyone can access the chain since it is open and distributed and it is not governed by any other third party or the organization.

CHAPTER 2

AIM AND SCOPE

AIM OF PROJECT

The traditional paper-based degrees and mark cards are vulnerable with fraud occurring through forgery and mistakes. Paper based mark sheet are inaccessible quickly, limited flexibility, lengthy process, high-cost and are non-eco-friendly. The students applying for jobs immediately after graduation, the students applying for abroad universities with an intention to pursue higher education and the recruiters are all facing problem with respect to mark sheet validation as fake mark sheet and degree certificates are rampant everywhere. So this paper intends to propose a system that eliminates the forgery of certificates.

Objectives

By using the unmodifiable property of blockchain provide more security. Confidentiality is transparent with each transaction visible to all the peers. Our application runs in offline mode. The certificate is validated rapidly. Provide accurate and reliable information.

SCOPE

Blockchain is a technology underlying the emerging cryptocurrencies including Bitcoin. The key advantage of blockchain is widely considered to be decentralization, and it can help establish disintermediary peer-to-peer (P2P) transactions, coordination, and cooperation in distributed systems without mutual trust and there is centralized control among individual nodes, based on such techniques as data encryption, time-stamping, distributed consensus algorithms, and economic incentive mechanisms. Blockchain can be called as the next generation of cloud computing, and is expected to radically reshape the behaviour model of individuals and organizations, and thus realize the transition from the Internet of Information today to the future Internet of Value. Blockchain is a distributed database that is widely used for recording 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 in the blockchain contains the hash value of its last counterpart for connection. All blocks in the

blockchain are connected and together they form a blockchain. Data is distributed among various nodes (the distributed data storage) and are thus decentralized. In the 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.

LITERATURE REVIEW

- The new Blockchain based system reduces the certificate forgery and ensures authentication, integration and security.
- Students demand a proof-of-certification at low cost and easy to check, employers also demand quick and trustable verification of degrees when recruiting.
- Digital certificates are registered on the Bitcoin blockchain, cryptographically signed, and tamper-proof. A certificate issuer signs a well-structured digital certificate and stores its hash within a blockchain transaction. Transaction output is assigned to the recipient.
- The Blockchain hash function offers a better strategy for signature preservation. Blockchain adoption is more advantageous to records with a permanent retention schedule.
- Jin-chiou et al developed software in order to avoid counterfeiting certificates. Due to the lack of an anti-forge mechanism, the graduation certificate is to be forged. So, the decentralized application was designed based on Hyperledger blockchain technology. First, generate the digital certificate for the paper certificate then hash value created for the certificate is stored in the blockchain system. Even it used to verify the authenticity of the certificate it required another scanning app to scan the certificate. The system saves on paper, prevent document forgery. But the QR-Code must be scanned with a smartphone and an internet connection is required.
- Mandala et al used the Hyperledger Fabric blockchain platform. In this system, the certificates are issued by CAs only by obtaining approval from the domain owner Certificate Transparency (CT) technique, invented by Google. The aim to prevent SSL/TLS CA from issuing certificates for a domain without

visible to

the owner of the domain. But there was low scalability and less transaction. Aisong Zhang et al designed a system based on consortium blockchain technology. They used a secret sharing scheme. It can validate the digital certificate to protect the user's information and also the property of the user. The digital certificate revocation lists have collaborated among the CAs. The trust and reliable CRL (Certificate Revocation List) are more compared with the traditional system. If the user wants to verify the certificate, they only need to decrypt the signature with the public key. And the result will be compared with the hash operation of the original message. If the result is consistent, it proved that the digital certificate not tampered. But there is a false sense of security.

- Macro Baldi et al[5] designed a system named certificate validation through public ledgers and blockchain. In this system, CRLs(Certificate Revocation List) were distributed through the use of a private blockchain, and it shared among CA(certification authority).CAs are responsible for issuing certificates to requestors who meet the requirements and maintain CRLs. The certificate revocation list was available and authentication was provided at any time for a certificate. The certificate revocation list for a set of the certificate was maintained by the same certification authority who issued the certificates. CA ecosystem is fragile and prone to compromise.
- Marco Valdi, Franco Chiaraluce, Emanuele Frontoni, Luca Spalazzi(2017) 'Certificate validation through public ledger and blockchain' The project is proposed for the solution of addressing the issues of reliability and security of certificate revocation information. Its main advantages are in removing any single POF and being relatively simple to implement by leveraging existing open source platforms.
- Rujia Li, Yifan Wu(2016) 'Block chain based academic certificate authentication system' The project consists in designing and implementing by conflating the hash value of local files to the blockchain but remains numerous issues, did an effective technological approach protecting authentic credential certification and reputation appear.

CHAPTER 3

SYSTEM DESIGN & METHODOLOGY

EXISTING SYSTEM

In the current scenario, the certificates and mark sheets are stored in a centralized manner and verified manually, so it takes too much time to verify it. There is no safety to the certificates that are given to any private sector. The data may be changed, deleted, or modified. Certificates can be easily hacked and duplicates of that certificate can be made. When students bring their certificates to the interview, there is no security for certificates and the certificates or mark sheets might be modified. The certificate are stored in centralized manner and verified manually, so it takes too much time to verify. There is no safety to the certificate that are given to any private sectors (banks). But the data may be changed, deleted or modified. Certificates are easily hacked and make duplicate of that certificate. Students bring their certificates on interview places. There is no security for certificates.

PROPOSED WORK

Our proposed solution is that, instead of manually storing the mark sheets and certificates we can use blockchain technology for their storage. All the data in the blockchain will be stored using secure hash thus, making it more secure. Data once written in blockchain cannot be altered, hence the forgery of mark sheets will be reduced. Once the mark sheet data is written in blockchain it can be easily verified by university or any organization. Hyperledger Fabric will allow only approved participants to read and write on the student certificate. Moreover, blockchain technology ensures that all updating held are accurate and tamper-proof. The three main participants are University/Admin, student and verifier (the student allows to access). The Hyperledger workflow shows how the document is transferred. Suppose A wants to send a document to B, then A looks up his app for B's address on the network. The app looks up for membership services to validate B's membership. If B's membership is found then the Hyperledger network connects both the parties directly affiliated with the deal. Both parties generate a result which is then sent to the consensus cloud to be ordered and verified. Once the consensus

cloud validates the transaction.

SYSTEM DESIGN

The student's achievements available in the form of degree certificate, mark sheet, value added certificate, etc., will become an important weightage for recruitment or higher studies. The Education institution awards and degree certificates may have only the names of the institution and the student's data. In this scenario there is a lack of effective anti-forgery mechanism, due to these events many times the graduation certificate to be forged often is found. To solve the problem of fake certificates, the blockchain technology would store the certificate in digital form. The immutability nature of blockchain makes digital certificate in the distributed ledger is very difficult to tamper or modify also it is very easy to verify the originality of digital certificate.

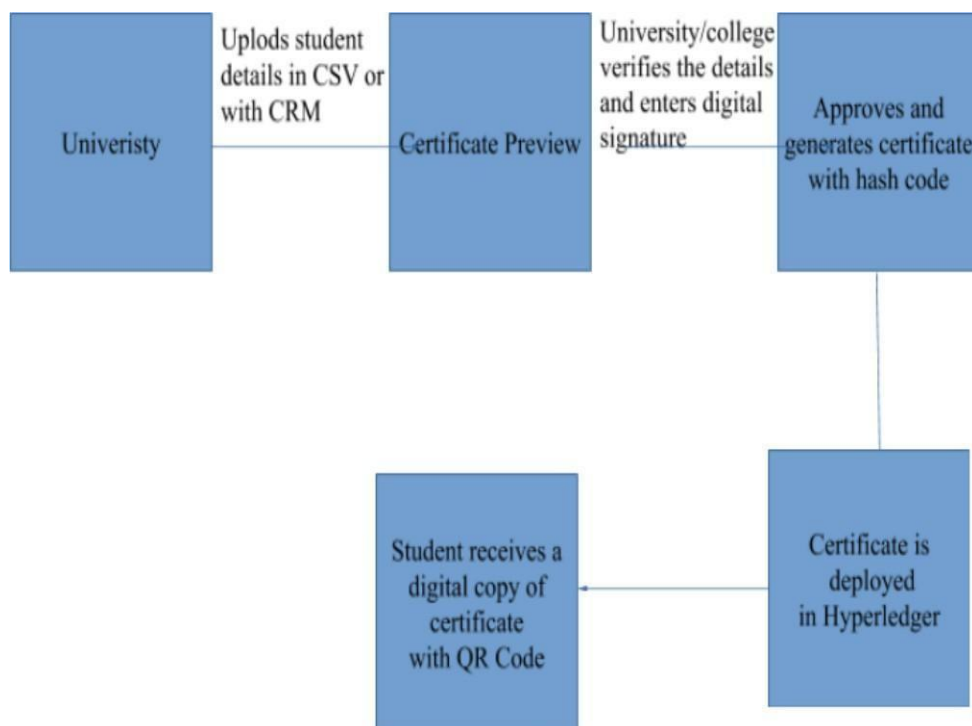


Fig: 3.1 System Design

The university or admin uploads the student details. Only the admin/university can make changes in the certificate and other details. The details that the admin entered will be moved to the Hyperledger fabric. We cannot directly connect to the Hyperledger fabric, it will be done via composer Rest Server. The fig.3 shows the process flow diagram of certificate issuance. When the admin an account, full details

of student is getting stored. Then creates a certificate preview, the university verify that and enters

the digital signature. Then generates a hash code. The approved certificate is deployed in Hyperledger.

PROCESS

The process of issuing digital certificates in the system is as follows. First step, generate the hash value for certificate using double SHA256. Store the fixed length hash value as a transaction in the block. This transaction is validated by the members in the blockchain, once it is trusted as valid transaction then the block is added with existing blockchain. Accepting and rejecting will be done using consensus algorithm. The consensus algorithm may be chosen based on number of nodes, and transactions. The system will generate the related QR code and inquiry string code to affix in the hardcopy certificate. The system provides the unit to authenticate the hardcopy certificate through phone scanner or website. The immutability nature of the distributed ledger, the system provides not only verification of certificate and also it stores the certificate in digital form forever [10]. The certificate is stored in JSON and pdf format. The pdf copy is uploaded to inter planetary file system node and the hash pointer is saved. The JSON file is imported by Hyperledger to create an asset. IPFS is a peer-to-peer distributed file system that seek to connect the computing devices with the same system of files. Third party verifier is one of our participants. By using this system, the verifier can easily verify without any difficulties. The verifier receives a QR code from student, using that the verifier can view the certificate. All the history of student mark list is recorded. So, without any doubt the verifier can easily understand.

CHAPTER 4

SOFTWARE DEVELOPMENT METHODOLOGY

REQUIREMENT SPECIFICATION

The Hyperledger fabric is a infrastructure which is supported by Hyperledger Composer. Hyperledger Composer is one of the open-source project and a tool for implementing blockchain frameworks. It helps the existing networking system to cooperate easily with a new decentralized platform.

- Simple Modelling Language – nodejs.
- The platform offers production-ready POCs that saves time and all of them are reusable.
- Data Integration – Loopback feature.

Hardware Requirements

- Processor : Intel® Core™ i5 above/ Ryzen 5 above
- RAM : 8.00GB above
- Hard Drive : 1TB

Software Requirements

- Operating system : Ubuntu Linux 14.04 / 16.04 LTS
- Framework : Hyperledger Fabric
- Tools : Hyperledger Composer
- Docker engine : version 17.03 or higher
- Docker Composer : version 1.8 or higher
- Code Editor : Visual Studio Code
- Programming language : Go or Nodejs

BLOCKCHAIN

Blockchain is one of the latest technologies, which enables new forms of distributed software architecture. The blockchain data structure is a time-stamped list of blocks, which records and aggregates data about transactions that have ever occurred within the blockchain network. The blockchain provides an immutable data storage, which only allows inserting transactions without updating or deleting any existing transaction on the blockchain to prevent tampering and revision. Each transaction can be separately verified by using its hash value, since it is open, publicly verifiable and the data once entered cannot be altered which help in preventing forgery. In blockchain each block of transactions is linked to the previous block by the hash value of preceding block. Blockchain technology was first introduced as an underlying technology of cryptocurrency Bitcoin. Bitcoin, an electronic payment system, is launched in order to solve the problem of centralization in current payment systems i.e., banks, financial institutions etc., where a central authority is the only authoritative party who is in charge of processing the electronic payments.

FEATURES OF BLOCKCHAIN

The main features of blockchain technology are:

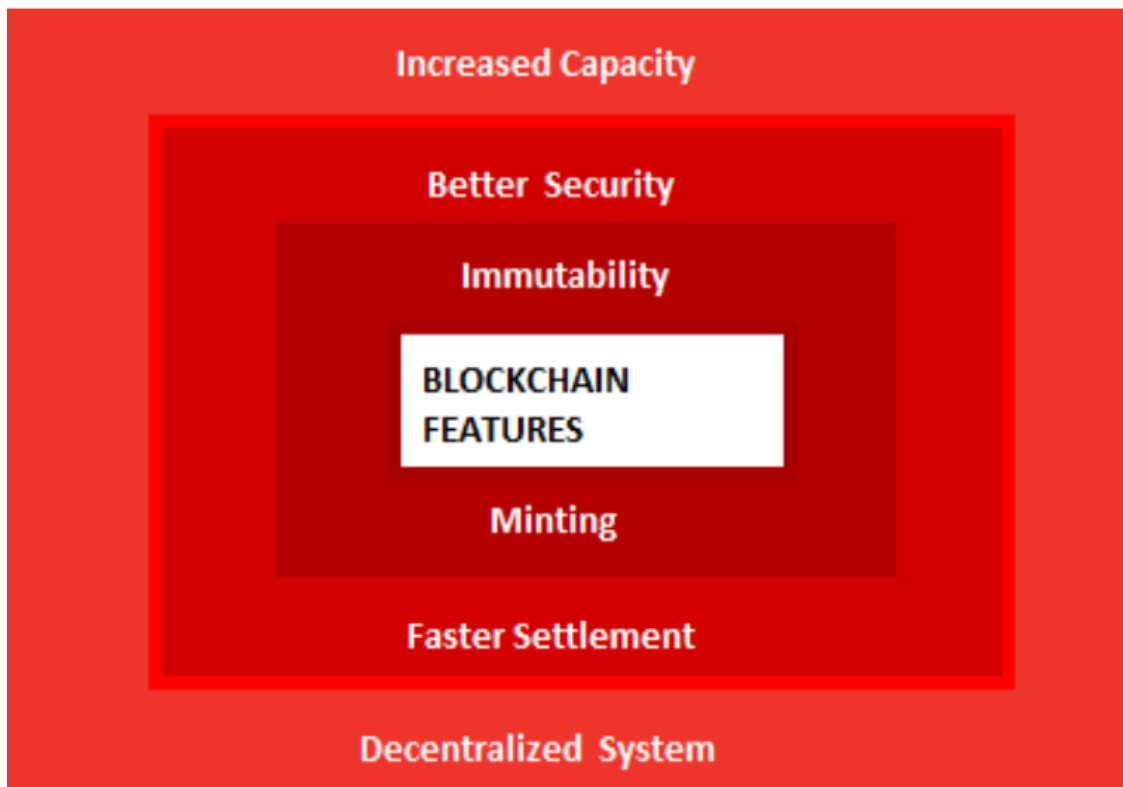


Fig: 4.1 Features of Blockchain

Increased Capacity

It increases the capacity of the whole network, since there are lot of computers working together which offers a great power in total then few of the devices where the things are centralized.

Better Security

There is no chance of shutting down of the system since Blockchain technology has a better security. The main reason is that the Blockchain network is secured by a number of computers called nodes and transaction on this network is confirmed by these nodes.

Immutability

One of the main values of Blockchain is creating immutable ledgers. The databases which are centralized are most likely to get hacked and to keep these databases secure they require trust in the third party.

Faster Settlement

A lot of settlement time is required, which usually takes days to proceed may cause the traditional banking systems to slow down. Because of this reason these banking institutes needs to upgrade their banking systems. With the help of Blockchain technology we can solve this problem as it can settle money transfer at really fast speeds. It provides convenience to the consumers since it saves a lot of time and money from these institutions.

Decentralized System

The decentralized technology gives the power to store assets in a network which further accesses by the means of the internet. An asset can be like a document, a contract, etc. By this the owner can have a direct control over his account which gives the owner a power to transfer his assets to anyone he wants to by the means of a Key that is linked to his account.

Minting

By help of the Blockchain we can solve the various ways of minting a problem of manipulation. The role of the miner is to create a block for many new methods which has also been introduced as proof of work is the approach by which an individual can prove that he is engaged in a significant amount of computation work.

HYPERLEDGER

Hyperledger fabric is a distributed ledger technology. The main characteristics of Hyperledger fabric is, it is a permissioned network, it supports confidential transactions, to participate one doesn't need cryptocurrency and it is programmable. With these characteristics it establishes trust, Transparency and accountability. Three main concepts of Hyperledger includes asset, chain code and ledger. Asset is some kind of value which can be exchanged on blockchain system. On Hyperledger fabric asset representation be on Json or Binary format. Chain code defines the structure of asset and also defines the transactions. All transactions are recorded on a ledger. Ledger is a data structure, which tracks all of the asset transactions and it also records state changes of assets. All blockchain technologies have a concept of nodes, which is a communication entity. All nodes have a valid certificate. There are three types of nodes; peer (Keeps the ledger data in synch across network), client (initiates the transactions), orderers (responsible for distribution of transactions).

Membership service provider

All entities participate in Hyperledger fabric is known and have an identity which is assigned by way of certificates. Members are legally separate entities; these are the organizations that have decided to adopt blockchain for process automation. Each of these members are assigned a certificate and depending on the authority they may be able to use an MSP to create participant and infrastructure component identities within their organization. A blockchain network have more than one Membership service providers (MSP).

Certification Authority

Certification authority (CA) is a trusted third party that affirms the identity of an entity

by signing the certificate containing the entity's public key registration authority (RA) and the validation authority (VA). Fabric CA implementations have two parts: fabric

CA server and fabric CA client. Members issue their own identity within their organization. So, the Hyperledger fabric network can have one or more certification authority to manage the certificates. y. There are two other authorities that are referred in the context of CA are the

Business Network

Cards Business network card contain the configuration information that is needed by the tools and applications for connecting to the business network applications and the Hyperledger infrastructure components. There are two administration roles for the BNA; peer admin and network admin. Peer admin creates the network admin and the network admin creates different participants in BNA. The business network card contains the credentials and the composer connection profile. Composer CLI is used for managing the cards.

Fabric Composer

A composer is an open development toolset/framework which makes it easy for creation and management of business network application. The primary goal is to accelerate the development of blockchain applications on Hyperledger. The benefits of using Hyperledger composer are it reduces the time to value, it hides the complexity of underlying infrastructure, easy to develop smart contracts and it offers business modelling capability. Many tools are available in the toolset like tools for developers, operations, administrators and business analyst.

SMART CONTRACTS AND CHAINCODE

From an application developer's perspective, a smart contract, together with the ledger, form the heart of a Hyperledger Fabric blockchain system. Whereas a ledger holds facts about the current and historical state of a set of business objects, a smart contract defines the executable logic that generates new facts that are added to the ledger. A chain code is typically used by administrators to group related smart contracts for deployment, but can also be used for low level system programming of Fabric. In this topic, we'll focus on why both smart contracts and chain code exist, and how and when to use them. Chain code is a program, written in Go, node.js, or Java that implements a prescribed interface. Chain code runs in a secured

Docker container isolated from the endorsing peer process. Chain code initializes and manages ledger state through transactions submitted by applications.

A chain code typically handles business logic agreed to by members of the network, so it may be considered as a “smart contract”. State created by a chain code is scoped exclusively to that chain code and can't be accessed directly by another chain code. However, within the same network, given the appropriate permission a chain code may invoke another chain code to access its state.

NODEJS

Node.js is a server-side platform built on Google Chrome's JavaScript Engine (V8 Engine). Node.js was developed by Ryan Dahl in 2009 and its latest version is v15.11.0. Node.js is an open source, cross-platform runtime environment for developing server-side and networking applications. Node.js applications are written in JavaScript, and can be run within the Node.js runtime on OS X, Microsoft Windows, and Linux.

Node.js also provides a rich library of various JavaScript modules which simplifies the development of web applications using Node.js to a great extent.

Features of Node.js

Following are some of the important features that make Node.js the first choice of software architects.

- **Asynchronous and Event Driven** – All APIs of Node.js library are asynchronous, that is, non-blocking. It essentially means a Node.js based server never waits for an API to return data. The server moves to the next API after calling it and a notification mechanism of Events of Node.js helps the server to get a response from the previous API call.
- **Very Fast** – Being built on Google Chrome's V8 JavaScript Engine, Node.js library is very fast in code execution.

- **Single Threaded but Highly Scalable** – Node.js uses a single threaded model with event looping. Event mechanism helps the server to respond in a non-blocking way and makes the server highly scalable as opposed to traditional servers which create limited threads to handle requests. Node.js uses a single threaded program and the same program can provide service to a much larger number of requests than traditional servers like Apache HTTP Server.
- **No Buffering** – Node.js applications never buffer any data. These applications simply output the data in chunks.
- **License** – Node.js is released under the MIT license.

Fabric-Contract-API

The fabric-contract-api provides the contract interface a high-level API for application developers to implement Smart Contracts. Working with this API provides a high-level entry point to writing business logic. Within Hyperledger Fabric, Smart Contracts can also be referred to as Chain code. To be more specific, the term chain code is preferred to be used to refer to the overall container that is hosting the contracts. The fabric-shim provides the chain code interface, a lower-level API for implementing "Smart Contracts". It also currently provides the implementation to support communication with Hyperledger Fabric peers for Smart Contracts written using the fabric-contract-api. To confirm that this is the same as the fabric-shim in previous versions of Hyperledger Fabric.

Fabric-Shim

The fabric-shim provides the chain code interface, a lower-level API for implementing "Smart Contracts". To confirm that this is the same as the fabric-shim in previous versions of Hyperledger Fabric.

GO PROGRAMMING

Go language is a programming language initially developed at Google in the year

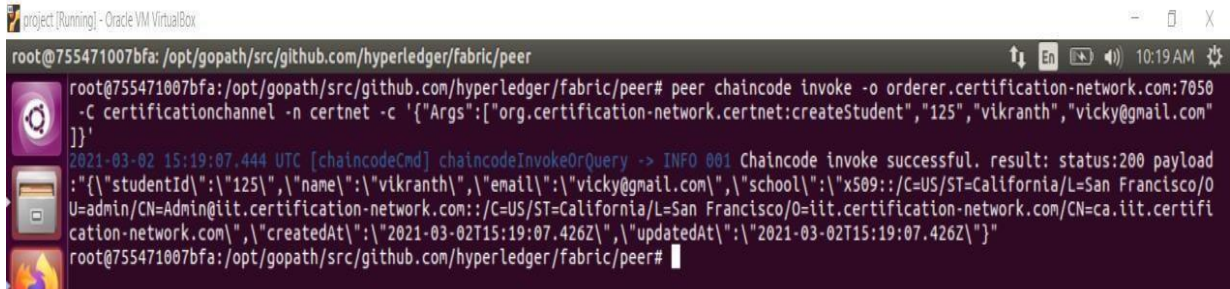
2007 by Robert Griesemer, Rob Pike, and Ken Thompson. It is a statically-typed language

having syntax similar to that of C. It provides garbage collection, type safety, dynamic- typing capability, many advanced built-in types such as variable length arrays and key- value maps. It also provides a rich standard library. The Go programming language was launched in November 2009 and is used in some of the Google's production systems. **Go** is a procedural programming language. It was developed in 2007 by Robert Griesemer, Rob Pike, and Ken Thompson at Google but launched in 2009 as an open-source programming language. Programs are assembled by using packages, for efficient management of dependencies. This language also supports environment adopting patterns alike to dynamic languages.

CHAPTER 5

RESULTS AND DISCUSSION

CREATING STUDENT



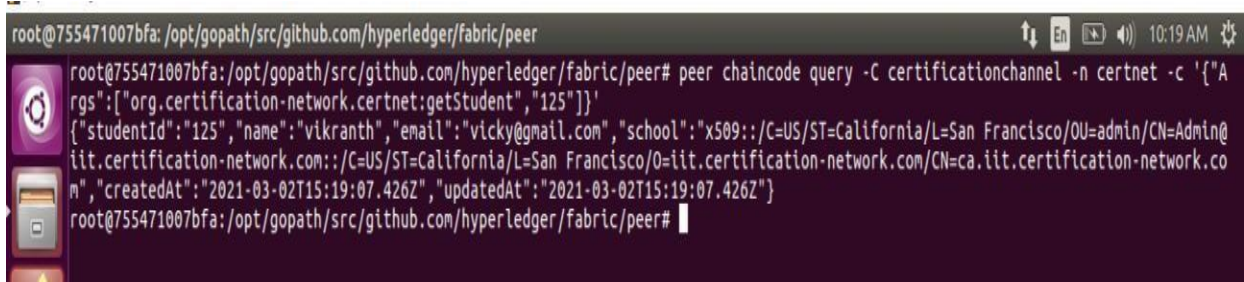
```
root@755471007bfa: /opt/gopath/src/github.com/hyperledger/fabric/peer
root@755471007bfa:/opt/gopath/src/github.com/hyperledger/fabric/peer# peer chaincode invoke -o orderer.certification-network.com:7050
-C certificationchannel -n certnet -c '{"Args":["org.certification-network.certnet:createStudent","125","vikranth","vicky@gmail.com"]}'
2021-03-02 15:19:07.444 UTC [chaincodeCmd] chaincodeInvokeOrQuery -> INFO 001 Chaincode invoke successful. result: status:200 payload
:{"studentId":"125","name":"vikranth","email":"vicky@gmail.com","school":"/C=US/ST=California/L=San Francisco/O
U=admin/CN=Admin@iit.certification-network.com:/C=US/ST=California/L=San Francisco/O=iit.certification-network.com/CN=ca.iit.certifi
cation-network.com","createdAt":"2021-03-02T15:19:07.426Z","updatedAt":"2021-03-02T15:19:07.426Z"}
root@755471007bfa:/opt/gopath/src/github.com/hyperledger/fabric/peer#
```

Fig: 5.1 Creating Student

We create the student using “createStudent” function and give the name as “Vikranth” and roll no as “125” and Email as “vicky@gmail.com” and get the output as JSON file with name, student ID, email, school, createdAt and updatedAt in json file and save in ledger print the output.

We have syntax for creating student details “peer chaincode invoke -o orderer.certification-network.com:7050 -C certificationchannel -n certnet -c '{"Args":["org.certification-network.certnet:createStudent","0001","Aakash Bansal","connect@aakashbansal.com","15"]}'” we have –C means channel name. Name of the channel is certificationchannel. –n means name of the chaincode, name of chaincode is certnet –o is giving the orderer node, orderer.certification-network.com:7050 orderer and port number. We use “createStudent” and we create the student details.

GET STUDENT



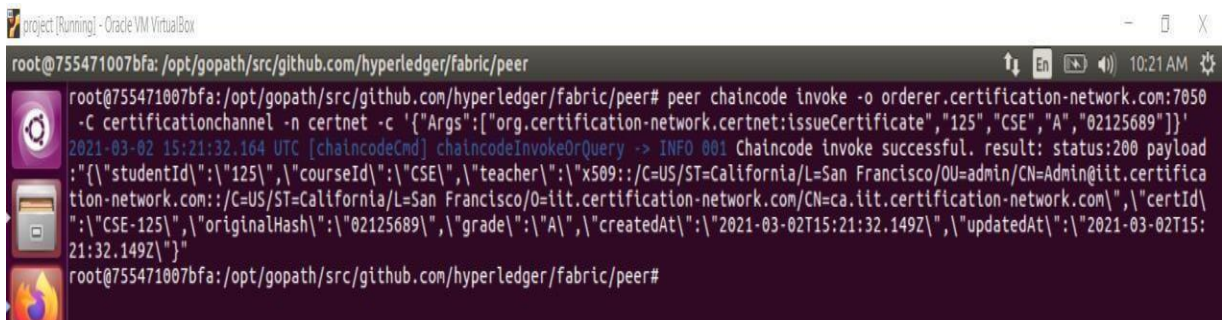
```
root@755471007bfa: /opt/gopath/src/github.com/hyperledger/fabric/peer
root@755471007bfa:/opt/gopath/src/github.com/hyperledger/fabric/peer# peer chaincode query -C certificationchannel -n certnet -c '{"Args":["org.certification-network.certnet:getStudent","125"]}'
{"studentId":"125","name":"vikranth","email":"vicky@gmail.com","school":"x509:/C=US/ST=California/L=San Francisco/OU=admin/CN=Admin@iit.certification-network.com:/C=US/ST=California/L=San Francisco/O=iit.certification-network.com/CN=ca.iit.certification-network.com","createdAt":"2021-03-02T15:19:07.426Z","updatedAt":"2021-03-02T15:19:07.426Z"}
root@755471007bfa:/opt/gopath/src/github.com/hyperledger/fabric/peer#
```

Fig: 5.2 Get Student

We can get the student details by using query statement we use the “getStudent” function for getting the student details we give the roll no as 125 and we the student details in json file with name, student ID, email, school, createdAt and updatedAt in json file and save in ledger print the output.

We gave the syntax for getting the student details “peer chaincode query -C certificationchannel -n certnet -c '{"Args":["org.certification-network.certnet:getStudent","0001"]}'". We have –C means channel name, name of the channel is certificationchannel. –n means name of the chaincode, name of chaincode is certnet –o is giving the orderer node. We use the “getStudent” for getting the student details from ledger.

ISSUE CERTIFICATE



```
root@755471007bfa: /opt/gopath/src/github.com/hyperledger/fabric/peer
root@755471007bfa:/opt/gopath/src/github.com/hyperledger/fabric/peer# peer chaincode invoke -o orderer.certification-network.com:7050 -C certificationchannel -n certnet -c '{"Args":["org.certification-network.certnet:issueCertificate","125","CSE","A","02125689"]}'
2021-03-02 15:21:32.164 UTC [chaincodeCmd] chaincodeInvokeOrQuery -> INFO 001 Chaincode invoke successful. result: status:200 payload:{"studentId":"125","courseId":"CSE","teacher":"x509:/C=US/ST=California/L=San Francisco/OU=admin/CN=Admin@iit.certification-network.com:/C=US/ST=California/L=San Francisco/O=iit.certification-network.com/CN=ca.iit.certification-network.com","certId":"CSE-125","originalHash":"02125689","grade":"A","createdAt":"2021-03-02T15:21:32.149Z","updatedAt":"2021-03-02T15:21:32.149Z"}
root@755471007bfa:/opt/gopath/src/github.com/hyperledger/fabric/peer#
```

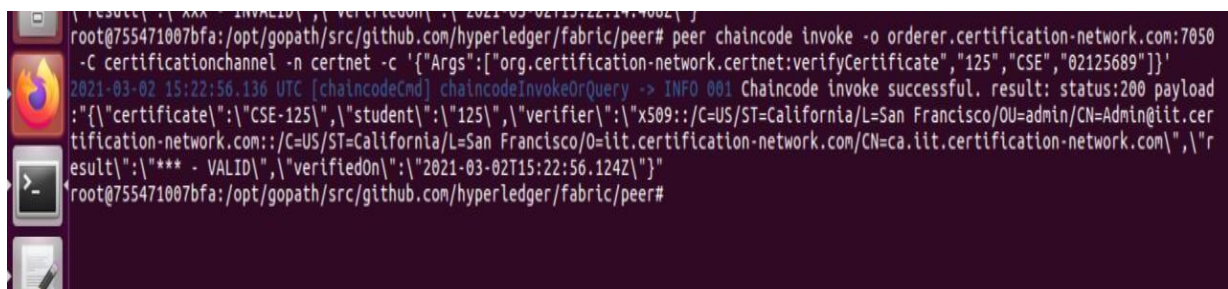
Fig: 5.3 Issue Certificate

We issue the certificate using “issueCertificate” function and give the Roll no as “125”, course id as “CSE”, grade as “A”, and original Hash as “02125689”. Get the

output as JSON file with student ID, course ID, Grade, original Hash, createdAt and updatedAt in json file and save in ledger print the output.

We have syntax for issue certificate details “peer chaincode invoke -o orderer.certification-network.com:7050 -C certificationchannel -n certnet -c '{"Args":["org.certification-network.certnet:issueCertificate","0001","0245","A","15569852"]}'” we have -C means channel name. Name of the channel is certificationchannel. -n means name of the chaincode, name of chaincode is certnet -o is giving the orderer node, orderer.certification-network.com:7050 orderer and port number. We use “createStudent” and we create the student details.

VERIFY CERTIFICATE



```
root@755471007bfa:/opt/gopath/src/github.com/hyperledger/fabric/peer# peer chaincode invoke -o orderer.certification-network.com:7050 -C certificationchannel -n certnet -c '{"Args":["org.certification-network.certnet:verifyCertificate","125","CSE","02125689"]}'
2021-03-02 15:22:56.136 UTC [chaincodeCmd] chaincodeInvokeOrQuery -> INFO 001 Chaincode invoke successful. result: status:200 payload:{"certificate":{"CSE-125"},"student":{"125"},"verifier":{"x509::C=US/ST=California/L=San Francisco/OU=admin/CN=Admin@iit.certification-network.com::C=US/ST=California/L=San Francisco/O=iit.certification-network.com/CN=ca.iit.certification-network.com"},"result":{"*** - VALID","verifiedOn":{"2021-03-02T15:22:56.124Z"}}}
root@755471007bfa:/opt/gopath/src/github.com/hyperledger/fabric/peer#
```

Fig:5.4 Verify Certificate

We issue the certificate using “verifyCertificate” function and give the Roll no as “125”, course id as “CSE”, grade as “A”, and original Hash as “02125689”. Get the output as JSON file with student ID, course ID, Grade, original Hash, result, createdAt and updatedAt in json file and save in ledger print the output.

We have syntax for verify certificate details “peer chaincode invoke -o orderer.certification-network.com:7050 -C certificationchannel -n certnet -c '{"Args":["org.certification-network.certnet:verifyCertificate","0001","0245","15569852"]}'” we have -C means channel name. Name of the channel is certificationchannel. -n means name of the chaincode, name of chaincode is certnet -o is giving the orderer node, orderer.certification-network.com:7050 orderer and port number. We use

“createStudent” and we create the student details.

CHAPTER 6

CONCLUSION AND FUTURE WORK

CONCLUSION

Using blockchain it is now possible to create a certification infrastructure that puts in record of our accomplishments. This allows us to share our credentials with respective validators. Now a days more researches based on different applications of blockchain are going on. For example in medical field, a healthcare record management system which will definitely be useful. We proposed a solution to the problem of certificate forgery based on blockchain technology. Providing security to the data is very important. By using the unchallengeable property of blockchain, we can provide more security for data and reduce the certificate forgery. The application can allow the user to view and validate the certificate. This system guarantees information accuracy and security and is easy for people to manage digital certificates.

FUTURE WORK

In future, the system for mark sheet verification can be modified by using smart contracts. Smart contracts are like digital protocols which are used to enforce a contract without any control from a third party. Smart contracts help to automatically compute the results eliminating illegal activities completely. Transparency and data immutability are the main features of blockchain application. It is a distributed ledger where nodes in the network validate and make final consensus to add the data in the network. The process of academic certificate generation is open and distributed among the parties where any organization or parties can verify information of any academic certificate using this blockchain system. The Ethereum blockchain also ensures data stored on blockchain network is encrypted, therefore only the certificate owner can see and share this data as they wish. In conclusion, academic institutions are able to collaborate with other employers and publish credentials on the blockchain to eradicate fake educational certificates.

REFERENCES

- [1]. Ruksudaporn Wutthikarn and Yan Guang Hui. "Prototype of Blockchain in Dental care service application based on Hyperledger Composer in Hyperledger Fabric framework", IEEE, Vol. 4, 2018.
- [2]. Tagrid Alshalali, Kenneth M'Bale D.Sc and Darsana Josyula Ph.D. "Security and Privacy of Electronic Health Records Sharing Using Hyperledger Fabric", International Conference on Computational Science and Computational Intelligence (CSCI), vol. 4, 2018.
- [3]. Osman Ghazali and Omar S. Saleh. "A Graduation Certificate Verification Model via Utilization of the Blockchain Technology", Journal of Telecommunication, Electronic and Computer Engineering., vol. 6, 2018.
- [4]. Jiin-Chiou Cheng, Narn-Yih Lee , Chien Chi , and Yi-Hua Chen. "Blockchain and Smart Contract for Digital Certificate", IEEE International Conference on Applied System Innovation, Vol. 6, 2018.
- [5]. S.Sunitha kumari¹ and D.Saveetha. "Blockchain and Smart Contract for Digital Document Verification", International Journal of Engineering & Technology, Vol. 4, 2018.
- [6]. Nitin Kumavat , Swapnil Mengade , Dishant Desai and JesalVarolia. "Certificate Verification System using Blockchain", International Journal for Research in Applied Science & Engineering Technology (IJRASET), Vol.7, issue .IV, April 2019.
- [7]. Yangpeng Zhu, Jiabao He, Kun Yuan and Yanmei Yang. "Research on Modify Protection of Metrology Electronic Certificate Based on Blockchain Technology", 14th International Conference on Computer Science & Education (ICCSE 2019).
- [8]. Stephen Thompson. "The preservation of digital signatures on the blockchain", the University of British Columbia iSchool Student Journal, Vol. 3 (2017).
- [9]. Binh Minh Nguyen, Thanh-Chung Dao and Ba-Lam Do. "Towards a blockchain-based certificate authentication system in Vietnam", PeerJ Comput. Sci. 6:e266 <http://doi.org/10.7717/peerj-cs.266.2020>.
- [10]. Marco Baldi, Franco Chiaraluce, Emanuele Frontoni, Giuseppe Gottardi,

Daniele Sciarroni and Luca Spalazzi. "Certificate Validation through Public Ledgers

and Blockchains”, in Proc. The First Italian Conference on Cybersecurity (ITASEC17), 2017

- [11]. R. L. Rivest, A. Shamir, L. Adleman, A method for obtaining digital signatures and public-key cryptosystems, Communications of the ACM, v.21 n.2, p.120-126, Feb. 1978
- [12]. Ouaddah, A. A. Elkalam, and A. A. Ouahman, “Towards a novel privacy-preserving access control model based on blockchain technology in IoT,” in Europe and MENA Cooperation Advances in Information and Communication Technologies. Springer, 2017, pp. 523– 533.
- [13]. J. van Beusekom, F. Shafait, and T. M. Breuel, “Text-line examination for document forgery detection,” Int. J. Doc. Anal. Recognit., vol. 16, no. 2, pp. 189– 207, 2013.
- [14]. M. Singh and D. Garg, “Choosing best hashing strategies and hash functions,” Int. Advance Computing Conf., 2009, pp. 50 – 55
- [15]. Samit Shivadekar (IT, SIES GST, Navi Mumbai, India,) Stephen Raj Abraham (IT, SIES GST, Navi Mumbai, India,) Sheikh Khalid (IT, SIES GST, Navi Mumbai, India), “Document Validation and Verification System”, International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 5 Issue 3, March 2016
- [16]. Anoukh. N, " Block Chain System for Data Management", International Journal of Financial Management (IJFM) Vol. 08, Issue 1, pp. 1-6, Jan 2019 [1].
S. Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, 2008; bitcoin.org/bitcoin.pdf.
- [17]. “Hyperledger project,” [online] Available: <https://www.hyperledger.org/> [Accessed on 5.07.2019]
- [18]. IBM Blockchain based on Hyperledger Fabric from the Linux Foundation.
Available from <https://www.ibm.com/blockchain/hyperledger.html>.
- [19]. Nachiappan Michael Crosby, Pradan Pattanayak, Sanjeev Verma, Vignesh Kalyanaraman, "BlockChain Technology: Beyond Bitcoin", Applied Innovation Review, no. 2, Jun. 2016.
- [20]. Tarek Kanan, Ahamd Turki Obaidat, Majduleen Al-Lahham, "SmartCert BlockChain Imperative for Educational Certificates", Electrical Engineering and

Information Technology (JEEIT) 2019 IEEE Jordan International Joint Conference on, pp. 629-633, 2019.

APPENDIX

A) PLAGIARISM REPORT

MARKSHEET VERIFICATION USING B...

ORIGINALITY REPORT

13%

SIMILARITY INDEX

7%

INTERNET SOURCES

10%

PUBLICATIONS

4%

STUDENT PAPERS

PRIMARY SOURCES

1

Ze Wang, Jingqiang Lin, Quanwei Cai,
Qiong Xiao Wang, Daren Zha, Jiwu Jing.
"Blockchain-based Certificate Transparency and
Revocation Transparency", IEEE Transactions
on Dependable and Secure Computing, 2020

Publication

4%

2

"Merged Papers", 2020 7th International
Conference on Smart Structures and Systems
(ICSSS), 2020

Publication

4%

3

dblp.dagstuhl.de

Internet Source

2%

4

www.irjet.net

Internet Source

2%

5

Submitted to Indian Institute of Technology,
Madras

Student Paper

1%

B) JOURNAL PAPER

MARKSHEET VERIFICATION USING BLOCKCHAIN

ABSTRACT

This record illustrates the utilization of blockchain innovation to forestall change of college tables. As per different examinations during the training time frame, understudies can get numerous declarations. Understudies will show these declarations while going after positions in account, wellbeing, innovation and numerous different fields, and every one of these testaments are needed for manual confirmation. Sometimes, understudies may show counterfeit endorsements, making it hard to recognize them. The issuance of phony instruction declarations has consistently been a drawn-out issue in the training area. Since such endorsements can be made effortlessly, and the validation interaction is exceptionally muddled on the grounds that they require manual check. This issue can be tackled by putting away the advanced authentication in the blockchain. Blockchain innovation gives predictable and openly ensured exchanges, and these blockchain designs can be utilized to make computerized against misrepresentation and simple to-demonstrated declarations.

INTRODUCTION

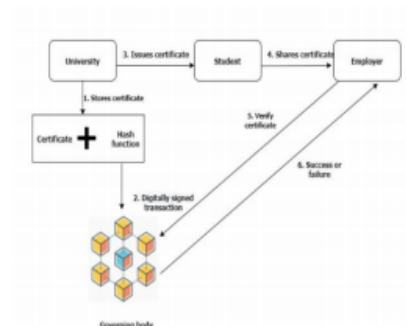
- One million individuals graduate every year. Graduation testaments and records contain individual data and ought not be effortlessly gotten to by others.
- Therefore, there is an incredible requirement for a machine to guarantee that the data in this record is genuine, which implies that the archive depends on an approved source and isn't fashioned.

- Verification of mark sheets is a tedious process for the industries to carry out, which often involves contacting the respective universities/colleges to cross verify the mark sheets.
- Any particular industry needs time to authenticate if the certificates of any student are genuine.
- In the blockchain, there is no centralized ledger but we use a decentralized ledger that means the same data is present with the members of that blockchain.

OBJECTIVES

- Verification of the marksheet using blockchain.
- We can verify the marks.
- We use blockchain for storing the data.

SYSTEM ARCHITECTURE



LITERATURE SURVEY

Blockchain and smart contract for digital certificate

As indicated by the Taiwan Ministry of Education, around 1 million understudies graduate every year, some of them will go to the nation, secondary school or school to proceed with their examinations, and some will be all set to attempt to find a new line of work. Over the span of the examination, different understudy testaments of competency, composing, certificates, and so forth, will be a significant pointer of admission to new schools or new openings. As the school will offer different honors or confirmations, just the name of the school and the understudy will be incorporated. Because of the absence of viable enemy of misrepresentation measures, graduation services frequently stand out. To take care of the issue of false authentications, a computerized confirmation framework dependent on blockchain innovation will be proposed. With non-convertible blockchain designs, a computerized endorsement with against phony and validation can be produced. The interaction for giving computerized endorsements to this program is as per the following. Initial, an electronic paper authentication record is made in the data set and other related data, and its hash esteem is determined all the while. At long last, the hash esteem is put away in the chain framework block. The program will produce the suitable QR code and inquiry code to connect to the paper declaration. It will be given to the unit that needs to confirm the realness of the paper endorsement by checking a mobile phone or a web question. By utilizing the perpetual blockchain structures, the framework not just builds the unwavering quality of different paper testaments, yet in addition mechanized the danger of losing different sorts of authentications.

Blockchain-based Certificate Transparency and Revocation Transparency

Traditional X.509 public key infrastructures (PKI) depend on a confided in certification authorities (CA) to sign the testament, which is utilized on SSL/TLS to validate the web worker and set up a safe channel. Nonetheless, late security occurrences demonstrate that the CA may (compromised) sign a phony authentication. In this article, we propose a reasonable exhibit of certificate transparency (CT) accreditation and revocation transparency (RT) to adjust the full CA authority. Our answer is consistent with the X.509 PKI, however we significantly improve the security of the endorsement. The title (ie web worker) distributes the marked CA testament of the SSL/TLS web worker with subtleties of its disintegration status as an exchange in a worldwide blockchain declaration. The blockchain declaration fills in as an extra open log for observing CA testament marking and execution, and gives the SSL/TLS web endorsement validation. The program thinks about the declaration acquired in SSL/TLS discussions with the testament in the public blockchain endorsement and possibly acknowledges it on the off chance that it has been given and the authentication has not been returned. We use Firefox and Nginx to utilize the model program, and test outcomes show that it presents all the more effectively.

Decentralized Digital Certificate Revocation System Based on Blockchain

The public key infrastructure (PKI) has been broadly used to make, oversee, disseminate, store and recover computerized authentications, which assume a significant part in coordinating secure interchanges. The PKI system

utilizes the relating public key to check business possession and establishes the framework for a public cryptographic key framework for public key encryption and advanced marks. Nonetheless, because of the presence of a focal certificate authority, the conventional PKi framework has security weaknesses, like a solitary mark of disappointment and assaults on intermediates. In this article, we survey the conventional PKi framework and existing security issues, and recommend potential answers for utilizing arising blockchain innovation to tackle these issues. Two structures are proposed in which the blockchain is utilized as a public notification board or a confided in larger part. We have left on the assignment of surveying the expense of time spent without demand and the expense of gas in that arrangement, demonstrating the achievability of the proposition and its viability.

MODULE DESCRIPTION

MODULE 1:

- In the module we can upload the marks of the students into the blockchain network.
- Blockchain is a decentralized network, tamper proof and cannot be manipulated.
- Only admin can add the marks of the students to the blockchain network.

MODULE 2:

- In this module the user can see the marks and verify the mark sheet.

- Anybody can verify the marks.
- Nobody can manipulate the data.

RESULTS AND DISCUSSION

- As you said, show the outcomes on a diagram or table
- Analyze and decipher the outcomes.
- Draw the conclusion.

CONCLUSION

- Explain the consequences of your undertaking
- Link your decisions to objectives.
- Describe future examination that you will most likely be unable to bear.

REFERENCES

1. Jiin-Chiou Cheng, Narn-Yih Lee, Chien Chi and Yi-Hua Chen, "Blockchain and Smart Contract for Digital Certificate", *IEEE International Conference on Applied System Invention (ICASI)*, 2018.
2. Z. Wang, J. Lin, Q. Cai, Q. Wang, J. Jing, D. Zha et al., "Blockchain-Based Certificate Transparency and Revocation Transparency" in *Financial Cryptography and Data Security. FC 2018, Berlin, Heidelberg:Springer*, vol. 10958, 2019.
3. D. S. V. Madala, M. P. Jhanwar and A. Chattopadhyay, "Certificate

- Transparency Using Computational Information
Blockchain", 2018 IEEE International Conference on Data Mining Workshops (ICDMW), pp. 71-80, 2018. Systems 7:5 (2011) pp.1582-1591.
4. Aisong Zhang and Xinxin Ma, "Decentralized Digital Certificate Revocation System Based on Blockchain", *Journal of Physics: Conference Series*, vol. 1069.
 5. J Tang, Xia Hu, Huiji Gao, Huan Liu, "Unsupervised Feature Selection for Multi-View Data in Social Media", *Proceedings of the ACM international conference on Information and Knowledge management* (2015), pp.1673-1678.
 6. Haytham Elzhazel and Alex Aulsebrook, "Unsupervised Feature Selection with ensemble learning ", *Machine Learning*, Springer (2013).
 7. Mohak Shah, Mario Marchand, and Jacques Corbeil, "Feature Selection with Conjunctions of Decision Stumps and Learning ", *IEEE TRANSACTIONS ON PATTERN ANALYSIS AND MACHINE INTELLIGENCE*, VOL. 34, NO. 1, (2012) pp.174-186.
 8. Qingzheng XU, Lei WANG, Baomin HE, Na WANG, "Modified Opposition-Based Differential Evolution for Function Optimization", *Journal of*

C) SOURCE CODE

Index.js

```
'use strict';

const certnetcontract = require('./contract.js');
module.exports.contracts = [certnetcontract];
```

contract.js

```
'use strict';

const {Contract} = require('fabric-contract-api');

class CertnetContract extends Contract {

    constructor() {
        // Provide a custom name to refer to this smart contract
        super('org.certification-network.certnet');
    }

    /* ***** All custom functions are defined below ***** */

    // This is a basic user defined function used at the time of
    // instantiating the smart contract
    // to print the success message on console
    async instantiate(ctx) {
        console.log('Certnet Smart Contract Instantiated');
    }

    /**
     * Create a new student account on the
     * network
     * @param ctx - The transaction context
     * object
     * @param studentId - ID to be used for
     * creating a new student
     *
     * @param name - Name of the student
     * @param email - Email ID of the student
     * @returns
     */
    async createStudent(ctx, studentId, name,
        email) {
        // Create a new
        // composite key for the
        // new student account
        const studentKey =
            ctx.stub.createCompositeKey('org.certification-network.certnet.student',
                [studentId]);

        // Create a student object to be stored in blockchain
        let newStudentObject = {
            studentId: studentId,
            name: name,
            email: email,
            school: ctx.clientIdentity.getID(),
            createdAt: new Date(),
        }
    }
}
```

```
        updatedAt: new Date(),  
    };  
  
    // Convert the JSON object to a buffer and send it to  
    blockchain for storage
```

```

        let dataBuffer =
Buffer.from(JSON.stringify(newStudentObject));
        await ctx.stub.putState(studentKey, dataBuffer);
        // Return value of new student account created to user
        return newStudentObject;
    }

    /**
     * Get a student account's details from the blockchain
     * @param ctx - The transaction context
     * @param studentId - Student ID for which to fetch details
     * @returns
     */
    async getStudent(ctx, studentId) {
        // Create the composite key required to fetch record from
blockchain
        const studentKey =
ctx.stub.createCompositeKey('org.certification-network.certnet.student',
[studentId]);

        // Return value of student account from blockchain
        let studentBuffer = await ctx.stub
            .getState(studentKey)
            .catch(err => console.log(err));
        return JSON.parse(studentBuffer.toString());
    }

    /**
     * Issue a certificate to the student after completing the course
     * @param ctx
     * @param studentId
     * @param courseId
     * @param gradeReceived
     * @param originalHash
     * @returns {Object}
     */
    async issueCertificate(ctx, studentId, courseId, gradeReceived,
originalHash) {
        let msgSender = ctx.clientIdentity.getID();
        let certificateKey =
ctx.stub.createCompositeKey('org.certification-
network.certnet.certificate',[courseId + '-' + studentId]);
        let studentKey =
ctx.stub.createCompositeKey('org.certification-network.certnet.student',
[studentId]);

        // Fetch student with given ID from blockchain
        let student = await ctx.stub
            .getState(studentKey)
            .catch(err => console.log(err));

        // Fetch certificate with given ID from blockchain
        let certificate = await ctx.stub
            .getState(certificateKey)
            .catch(err => console.log(err));

        // Make sure that student already exists and certificate
with given ID does not exist.
        if (student.length === 0 || certificate.length !== 0) {

```

```

        throw new Error('Invalid Student ID: ' + studentId +
' or Course ID: ' + courseId + '. Either student does not exist or
certificate already exists.');
```

```

    } else {
        let certificateObject = {
            studentId: studentId,
            courseId: courseId,
            teacher: msgSender,
            certId: courseId + '-' + studentId,
            originalHash: originalHash,
            grade: gradeReceived,
            createdAt: new Date(),
            updatedAt: new Date(),
        };
        // Convert the JSON object to a buffer and send it
to blockchain for storage
        let dataBuffer =
Buffer.from(JSON.stringify(certificateObject));
        await ctx.stub.putState(certificateKey, dataBuffer);
        // Return value of new certificate issued to student
        return certificateObject;
    }
}

/**
 * Verify Certificate
 * @param ctx
 * @param studentId
 * @param courseId
 * @param currentHash
 * @returns {Object}
 */
async verifyCertificate(ctx, studentId, courseId, currentHash) {
    let verifier = ctx.clientIdentity.getID();
    let certificateKey =
ctx.stub.createCompositeKey('org.certification-
network.certnet.certificate', [courseId + '-' + studentId]);

    // Fetch certificate with given ID from blockchain
    let certificateBuffer = await ctx.stub
        .getState(certificateKey)
        .catch(err => console.log(err));

    // Convert the received certificate buffer to a JSON object
    const certificate =
JSON.parse(certificateBuffer.toString());

    // Check if original certificate hash matches the current
hash provided for certificate
    if (certificate === undefined || certificate.originalHash
!= currentHash) {
        // Certificate is not valid, issue event notifying
the student application
        let verificationResult = {
            certificate: courseId + '-' + studentId,
            student: studentId,
            verifier: verifier,
            result: 'xxx - INVALID',
            verifiedOn: new Date()
        };
    }
}

```

```

        ctx.stub.setEvent('verifyCertificate',
Buffer.from(JSON.stringify(verificationResult)));
        return verificationResult;
    } else {
        // Certificate is valid, issue event notifying the
student application
        let verificationResult = {
            certificate: courseId
            + '-' + studentId,
            student: studentId,
            veri
            fi
            er
            :
            veri
            fi
            er
            ,
            re
            su
            lt
            :
            '*
            **
            -
            VA
            LI
            D'
            ,
            ve
            ri
            fi
            ed
            On
            :
            ne
            w
            Da
            te
            ()
        };
        ctx.stub.setEvent('verifyCertificate',
Buffer.from(JSON.stringify(verificationResult)));
        return verificationResult;
    }
}

module.exports = CertnetContract;

```