JAIN UNIVERSITY
Declared as deemed-to-be-University u/s 3 of the UGC act 1956

School of Engineering and Technology
Department of Information Science and Engineering
Jain Global Campus, Kanakapura Taluk - 562112
Ramanagara District, Karnataka, India

2017-2018

A Project Report on

"Decentralized Application for Digital Certification"

Submitted in partial fulfilment for the award of the degree of

BACHELOR OF TECHNOLOGY

IN

INFORMATION SCIENCE AND ENGINEERING

Submitted by

ARAVIND G
14BT1IS009

VARUN K
14BT1IS040

Under the guidance of

Ms. M S Sowmya
Assistant Professor
Department of Information Science and Engineering
School of Engineering & Technology
Jain University

December 2017

JAIN UNIVERSITY
Declared as deemed-to-be-University u/s 3 of the UGC act 1956

School of Engineering & Technology

Department of Information Science & Engineering

Jain Global campus
Kanakapura Taluk - 562112
Ramanagara District
Karnataka, India

CERTIFICATE

This is to certify that the project work titled **"Decentralized Application for Digital Certification"** is carried out by **Aravind G (14BT1IS009), Varun K (14BT1IS040),** bonafide students of Bachelor of Technology at the School of Engineering & Technology, Jain University, Bangalore in partial fulfillment for the award of degree in Bachelor of Technology in Information Science and Engineering, during the year **2017-2018**.

Ms. M S Sowmya	**Dr. Santosh Naik,**	**Dr. Hariprasad SA**
Assistant Professor	Head of the Department,	Director,
Dept. of IS&E,	Dept. of IS&E,	School of Engineering
School of Engineering &	School of Engineering &	& Technology,
Technology,	Technology,	Jain University
Jain University	Jain University	Date:
Date:	Date:	

Name of the Examiner Signature of Examiner

1.

2.

DECLARATION

We, **Aravind G (14BT1IS009), Varun K (14BT1IS040),** are students of Seventh Semester B.Tech in **Information Science & Engineering**, at School of Engineering & Technology, **Jain University**, hereby declare that the project titled **"Decentralized Application for Digital Certification"** has been carried out by us and submitted in partial fulfilment for the award of degree in **Bachelor of Technology in Information Science & Engineering** during the academic year **2017-2018**. Further, the matter presented in the project has not been submitted previously by anybody for the award of any degree or any diploma to any other University, to the best of our knowledge and faith.

Signature

Name: Aravind G
USN : 14BT1IS009

Name: Varun K
USN : 14BT1IS040

Place: Bangalore
Date :

ACKNOWLEDGEMENT

It is a great pleasure for us to acknowledge the assistance and support of a large number of individuals who have been responsible for the successful completion of this project work.

First, we take this opportunity to express our sincere gratitude to School of Engineering & Technology, Jain University for providing us with a great opportunity to pursue our Bachelor's Degree in this institution.

In particular we would like to thank ***Dr. Hariprasad****,* ***Director****,* ***School of Engineering & Technology****,* ***Jain University*** *for his constant encouragement and expert advice.*

It is a matter of immense pleasure to express our sincere thanks to ***Dr. Santosh Naik, Head of the department****,* ***Information Science & Engineering****,* ***Jain University,*** *for providing right academic guidance that made our task possible.*

We would like to thank our guide ***Ms. M S Sowmya, Assistant Professor****,* ***Dept. of Computer Science & Engineering****,* ***Jain University****, for sparing his/her valuable time to extend help in every step of our project work, which paved the way for smooth progress and fruitful culmination of the project.*

We would like to thank our Project Coordinator Mr. Saravana Balaji and all the staff members of Information Science & Engineering for their support.

We are also grateful to our family and friends who provided us with every requirement throughout the course.

We would like to thank one and all who directly or indirectly helped us in completing the Project work successfully.

Signature of Students

ABSTRACT

The rise of fraudulent cases seems to be a nuisance to organization as they're investment of money and various resources seem to be on someone who has false claims to. Verification process of these organizations was a long and tedious process where the organization would have lost of its time and resource on. Block chain technology was introduced fairly recently which is the underlying technology behind the very popular crypto currency Bitcoin. Blockchain is a decentralized, secure by design network which was designed to overcome double spending problem by a central server. The concept of central servers is eradicated in this architecture, where the data is distributed across geographically separated ledgers. Blockchain's applications diversified as MIT Media Labs introduced Blockcerts for certification of academic records. Ethereum is a platform for developing these decentralised applications using Blockchain ledgers. Etherum uses a concept called Merkle trees which is the concept behind verification through hashing. Based on the very same concept used by Blockcerts; this application would make verification of academic documents simple and quick with the usage of Blockchain client such as Ethereum and an IPFS hash. Despite various issues such as scalability and capital cost, these decentralized applications work in the favours of various organizations providing legitimacy, accuracy and security.

TABLE OF CONTENTS

LIST OF FIGURES

NOMENCLATURE USED

SFS	Self-certified file system
MOOC	Massive open online course
GUI	Graphical User Interface
DHT	Distributed Hash Table
EOA	Externally owned accounts

CHAPTER 1

CHAPTER 1

INTRODUCTION

One of the great promises of blockchain technology is that it can serve as a decentralized permanent unalterable store of all types of information or assets, not just as a currency or payment system. The project comprises of an application which would provide information about the certification of student's educational qualification which is digitally signed by the university/Education Board using blockchain technology. This is also applied to POA or POI documents as well. Similar to the idea of an E-Aadhaar but with a different use of technology.

1.1 Literature Survey

Despite the blockchain being in its initial stages, lot of applications and services are being rapidly developed. Services such as transfer of money, proof of consistency, proof of ownership, smart contracts and various other concepts. Blockchain is even will be used for voting in the distant future. But what concerns us the most is its robustness and immutability. Upon looking up these concepts enabled us to envision the project which can be used in any institution and alleviate many difficult processes.

Blockchain is the technology used behind the digital crypto currency known as Bitcoins. This technology was developed by a group known as Satoshi Nakamoto to solve the double spending problem which was problem of duplication/falsification. This paved way for a transaction without a trusted authority or a central server.

Web 3.0, a term coined for the change in the protocol of the Internet. At the moment, majority of the internet works on a centralized network where there is always a central server look after functions of the network. Since the introduction of bit coins, the technology behind it is being applied to the web as well. Decentralization is the key word here, which tells how Web 3.0 is totally a different path from the old Web 2.0. The protocols behind the new Web are in contrast with the old version, which means many applications are to be built from a scratch.

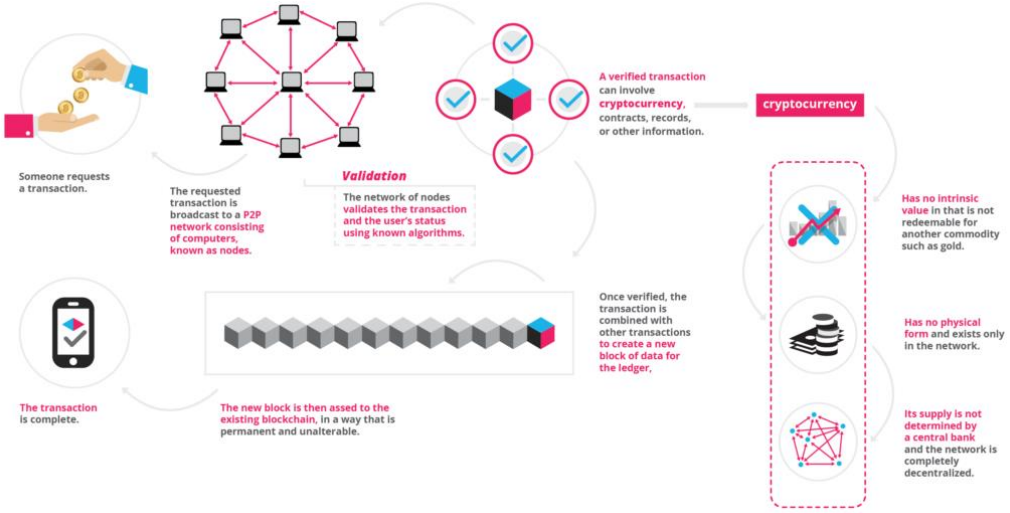

Fig. 1.1 Blockchain working.

Without the evolving internet many web applications had to upgrade to the emergence of the new technology. Tech giants such as IBM, Microsoft, Amazon, Infosys and many more have dwelled deep into this technology. Blockchain as a service (BaaS) has been initiated by cloud service providers, for instance this service is available on Bluemix by IBM, Amazon web services and even Microsoft Azure. This enables developers to build, test and deploy decentralised applications.

With such services already being provided, there is one such platform which is has been widely at the current point in time. This platform is called Ethereum. Ethereum is an important component in this report as we develop the application on this platform which shall be discussed further in the report.

Upon looking up the subject digital certification, one of most frequent occurring paper would be the MIT digital certificate paper. This provided the foundation to the application which we wanted to develop. This paper redirected to the new initiative which was undertaken by MIT known as Blockcerts.

This initiative was led by MIT Media Labs and Learning Machine. Learning Machine is a company which is solely dedicated to decentralising records which along with the partnership with MIT Media Labs co-created Blockcerts.

The above system architecture is based on the process by which Blockcerts function their digital certificates.

Blockcerts is an open source standard for digital certification. It is aligned with the following Decentralization and Data Signature standards.

- IMS Open Badges
- W3C Verifiable Claims
- W3C Linked Data Signatures
- W3C / Rebooting Web of Trust Decentralized Identifiers

With these standards Blockcerts assert that a viable application can be created on a decentralised system.

Maltese government have partnered with Learning Machine to provide digital academic certification allowing its people to store their academic qualifications and other records for free.

Holberton School, which was the first institution to issue digital certificates to students. Holberton School has partnered up with Bitproof, a company which is focused on producing digital certificates. This reported enabled employers to find at least 86% of the employee who lied in their resume. Bitproof also now provides developer tools to create certificates and also enable to develop blockchain applications as well.

Raman Technologies as well developed an academic digital certification as well. They have used the following stack for the development.

1.Ethereum Blockchain (Ethereum ropsten network)
2.PHP/AngularJS for web app development
3.Solidity smart contracts
4.IPFS distributed file storage
5.RabbitMq /whisper – messaging framework
6.PHP MVC for development of model view controller
7.PHP Laravel for RESTful web service framework
8.PKI and digital certificates (X.509 digital certificates)

Their application was based on Web applications and had expressed the desire enable this for Android and iOS.

The Humanized Internet, which includes a so-called identity-as-a-service, relying on the blockchain system. Blockchain offers an immutable, transparent, and distributed ledger that can provide a secure means of identifying every person on Earth. Think of blockchain as a universal, secure digital lockbox that could store information with your legal ID, such as property title, education certificates, and medical records, all in one place. The owner of the documents could access the system via mobile phone, and the identity could be confirmed using the owner's biometrics.

Sapien's Project was a digital certification project which focused on something little different. It focused on scalability of blockchain technology. They state that Lisk Sidechain would be able to provide SDK's for local computation which is less cost effective and scalable with high computation processes.

Proof of Existence, a blockchain based website which is used to prove the existence of a document. It was noted that some amount of money had to be paid as miner fee. Another observation was that word processing documents were not advisable. This is because word documents possessed metadata, the cryptographic digest generated is solely based on the document's content. So, the metadata of the document does not enable the blockchain to verify the existence of the document at the timestamp. This proves how exact the document must be for the blockchain to verify it. PDF and other unalterable format would be better for this usage.

1.2 Limitation of the current work

Currently our college has manual system of putting notices on notice board, which is out dated now. As expected, the current generation has no time to stand in rush in order to read the notices on notice board.

- Investment for decentralised ledgers.
- Requires maintenance and synchronization between servers.
- Requires more computation and increases network size.
- More complicated than usual server technologies.
- Immutability isn't always a boon.
- Transaction costs and network speed.

1.3 Problem definitions

Certificates are signals of achievement or membership and some are more important than others. University degrees (a particular type of certificate) can help you get the job you want, or prevent you from getting it if you don't have the right certificate. Our current, mostly analog system for managing certificates is slow, complicated, and unreliable. There are many advantages for creating a digital infrastructure for certificates, but the stakes are high since such a system could grow to represent our professional reputations. We need to be thoughtful about its design, and the type of institutions we trust to govern it.

Many aspirants like to pursue higher education at countries which specialize in a particular domain. Application to such universities requires document verification which is done by contacting the respective schools and colleges to provide confirmation about the applicant's qualification.

Similarly, in business companies perform background and educational verification of their employees. The reason behind such verification is that across the globe there are numerous fraudulent cases. Employee and students are found to have duped or lied in their resume about the certifications. This confirmation is done only done in the later stages of the verification process and would have given enough time for the fraudulent to have taken advantage over the company or university.

Time is wasted upon performing such tasks. On paper nothing seems to be believable unless confirmed by the board or institution. There are many such cases even in

India. For instance the Dr. BR Ambedkar University in Agra is alleged to have handed out thousands of fake degrees. Over 100s of fake degrees have been to relatives of the employees of the university. This wasn't confirmed until mid-2015.

A survey by one of the largest online job finder sites, CareerBuilder, shows that a staggering 58 percent of employers have caught a lie on a resume. The site has more than 23 million unique visitors and over 1.6 million jobs. Just over half of employers, 51 percent said that they would automatically dismiss a candidate once caught. Only seven percent said they would be willing to overlook a lie, if they liked the candidate. The HireRight report revealed that 50% of employers check education verification

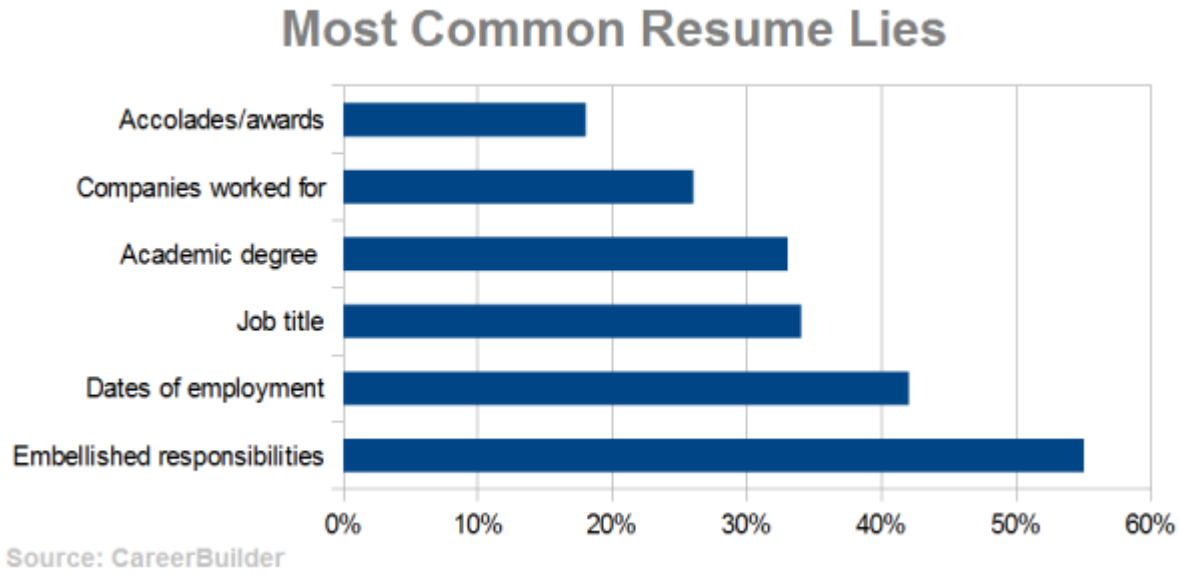

Fig. 1.2 Statistics of lies in Resume.

From Fig.1.2, we can notice that over 30% of the resume lie are academic degree. To prevent such fraudulent cases and also provide an ease of presentation of information to the respective organization is one of the reasons behind such a project.

1.4 Objectives

The main objective is to propose this system in our college to overcome listed limitations of manual notice work. The following are some of the advantages that can be expected through this application.

- **Development of decentralized application to issue and verify blockchain-based official records for academic credentials:**
  The main objective to go away from traditional centralized mechanism for verification and issuance of certificates to a decentralized and more secure mechanism using block chain.
- **Digitally accurate records of individual:**
  Block chain technology enables legitimacy and accuracy of the academic by verifying with the source of the document which is held by the university.
- **Secure and immutable information of the user.**
  Blockchain has security build within is architecture because of decentralization of the servers geographically, the threats which affect it are almost nil.
- **Use the convenience of smart phones for document submission:**
  Webapps can be accessed through the internet. Smart phones have the ability to access the internet which allows the application to work on phones as well.

CHAPTER 2

CHAPTER 2

Proposed system

2.1 Introduction

Depending on the results of the initial investigation, the survey is expanded to a more detailed feasibility study. Feasibility study is a test of system proposal according to its work ability, impact on the organization, ability to meet user needs, and effective use of resources. The objective for this phase is not to solve the problem but to acquire a sense of scope. During the study, the problem definition is crystallized and aspects of the problem to be included in the system are determined.

Decentralized Application Development Systems are capital investments because resources are being spent currently in order to achieve benefits to be received over a period of time following completion. There should be a careful assessment of each project before it is begun in terms of economic justification, technical feasibility, operational impact and adherence to the master development plan. We started the project by listing the possible queries that the user might want to be satisfied. And on these lines we took the project further.

The three main points, kept in mind at the time of project, are:

- Possible (To build it with the given technology and resources)
- Affordable (given the time and cost constraints of the organization)
- Acceptable (for use by the eventual users of the system)

The three major areas to be considered while determining the feasibility of a project are:

I. **Technical Feasibility:** The technical issue usually raised during the feasibility stage of the investigation includes the following:

- Does the necessary technology exist to do what is suggested?
- Does the proposed equipment have the technical capacity to hold the data required to use the new system?

- Will the proposed system provide adequate response to inquiries, regardless of the number or location of users?
- Can the system be upgraded if developed?
- Are there technical guarantees of accuracy, reliability, ease of access and data security?

Earlier no system existed to cater to the needs of Secure Infrastructure Implementation System. The current system developed is technically feasible. It is a web based user interface. Thus it provides an easy access to the users. The databases purpose is to create, establish and maintain a work- flow among various entities in order to facilitate all concerned users in their various capacities or roles. Permission to the users would be granted based on the roles specified. Therefore, it provides the technical guarantee of accuracy, reliability and security. The software and hardware requirements for the development of this project are not many and are already available as free as open source. The work for the project is done with the current equipment and existing software technology. Necessary bandwidth exists for providing a fast feedback to the users irrespective of the number of users using the system.

II. **Operational Feasibility:** Under this category of service we conduct a study to analysis and deter-mine whether user needs can be fulfilled by using a proposed solution. The result of our operational feasibility Study will clearly outline that the solution proposed for user business is operationally workable and conveniently solves user problems under consideration after the proposal is implemented. We would precisely describe how the system will interact with the systems and persons around. Our feasibility report would provide results of interest to all stakeholders. It will do as per the needs of the business requirements.

III. **Timeline Feasibility:** It is important to understand that a need must be fulfilled when it has to be. Some otherwise feasible and highly desirable projects can become non-feasible due to very restrictive timeline constraints. This fact makes it imperative that milestones are clearly linked to the timeline and projects are well conceived with safe unforeseen margins. We make sure that we strictly follow what has been stated above.

2.2 Architecture

2.2.1 System Architecture

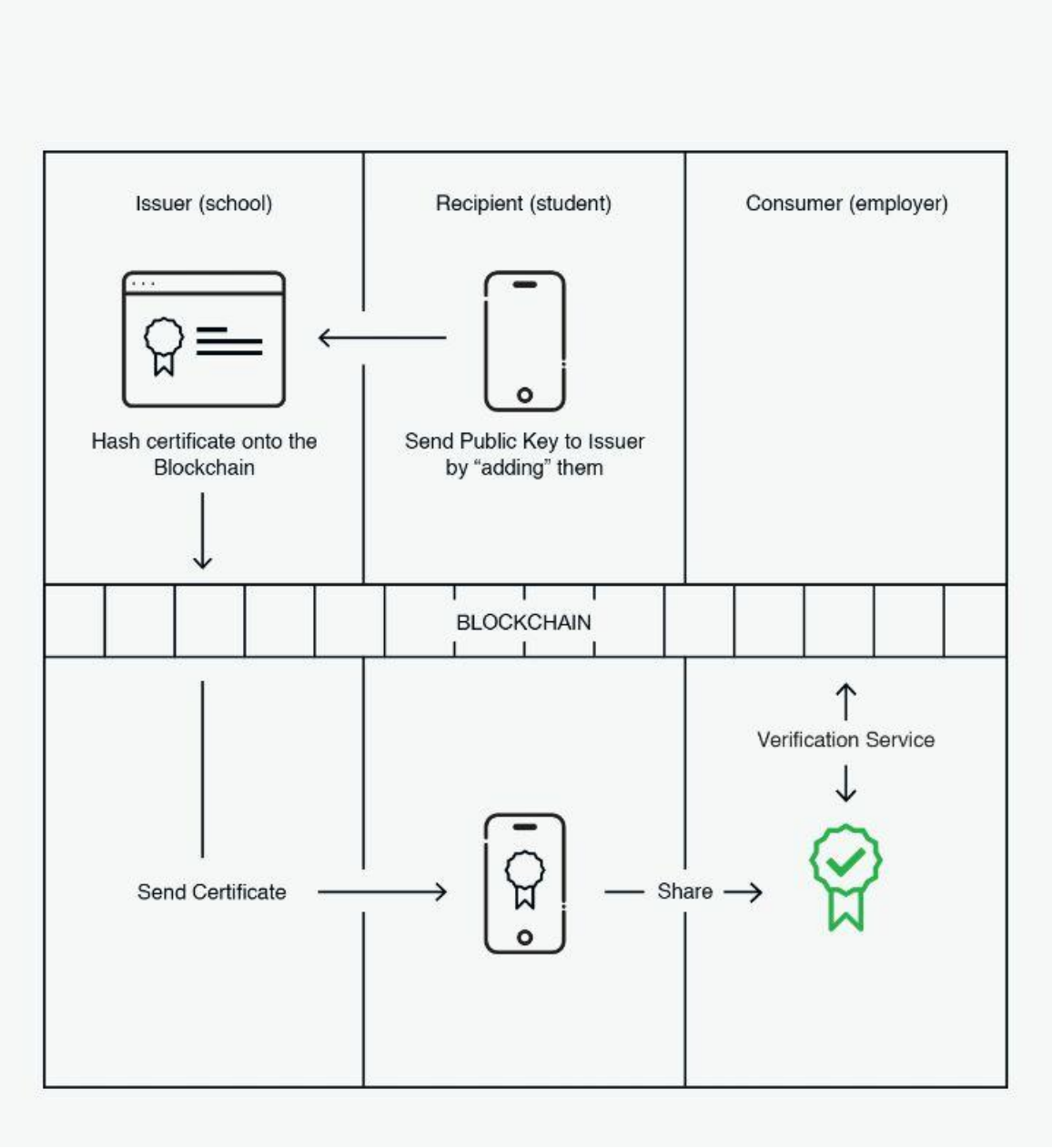

Fig.2.1 Architecture of proposed system

The Fig.2.1 above gives us a brief understanding of how the system functions. Let's discuss this in more brief terms without much technicality.

- Firstly the recipient (student), requests the University for his/her certificate through the application interface.
- Next, the university receives this notification and a certificate is generated along with a unique hash digest based on its contents such as USN.
- This certificate along with the digest is shared with the recipient who submits it to the respective consumer (employer).
- The consumer can verify the certificate using a third party application such as cert-verifier.

2.2.2 Data Requirements

The data required for the functioning of the application is the user's details which enables authentication of the user in the cert-wallet. The certificate is a data which is produced by the university along with a unique hash digest with which provides the required legitimacy for what the user is sharing to the client.

2.2.2 Functional Requirements

Some functional requirements which enable the application to fulfil its goals.

- ***User registration:***

  The student must register on a cert-wallet interface to ensure his/her usage on this application for authorization and authentication.

- ***User Login:***

  The registered user must use the credentials provided to be able to access his/her cert-wallet interface which enables the recipient to communicate with the issuer and share the certificate to the consumer.

- ***Wallet Inbox Interface:***

  Since there is a communication between the issuer and recipient for the certificate, an inbox type interface maybe to required to share information between each other.

2.2.3 System Dependability

The System depends some factors which are listed below.

- ***Internet Accessibility:***

  The system is based on block chain which is distributed geographically in different places and usage of a client such as Ethereum. Therefore to provide communication for such a system Internet access is a pivotal requirement.
- PDF or any immutable document viewer for displaying of the certificate.
- Web browser to access the application which is present in the web.

2.2.4 Maintainability Requirements

Following are the maintainability requirement for the application:

- ***Application extendibility:*** The application should be easy to extend. The code should be written in a way that it favours implementation of new functions. It is requires in order for future functions to be implemented easily to the application.
- ***Application testability:*** Test environments should be built for the application to allow testing of the applications different functions.

2.2.5 Look and Feel Requirements

Regarding look and feel, our client is straight forward. They believe in simplicity. So these are their requirements:

- ***Simple and Light:***

  The user interface should be simple and lightly coloured. It should give relaxing effect on looking at its GUI. No bright colours should be used while designing the UI of this application.
- ***Easy to Use***

  The application should be easy to use. If any user is doing something wrong, he/she should be informed correctly about what is going wrong behind the scenes. There should be proper instructions for the user to use this application.

2.3 Methodology

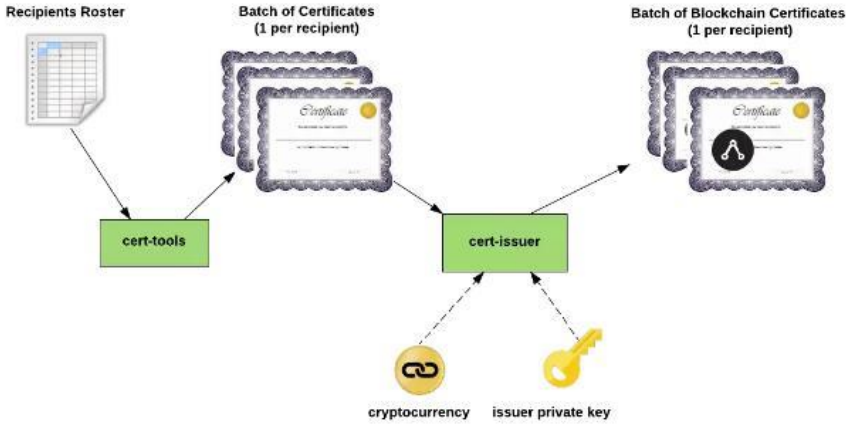

Fig.2.2 Workflow of Proposed system

As the Fig.2.2 mentions, initially the user whose certificate is to be verified sends a public key to the issuer. The issuer in our case is the University who provides validation of a student's educational qualification in that university. Basically, the student requests the School/University to issue his/her certificate.

This sharing of certificate is performed by using a certificate wallet which is in simple terms an interface.

The school/university then issues the certificate through the blockchain. This is done by performing a transaction on the bitcoin blockchain. Along with the certificate the issues adds the hash or the digest of the certificate.

Upon receiving the certificate, the recipient shares it with the Employer using a cert-wallet or even cert-viewer. cert-viewer is similar to the cert-wallet which acts an interface to view/display the certificate shared by the recipient.

To ensure the credibility of the certificate, the employer may use a third-party application to verify the certificate. This is done using a cert-verifier which uses the digest or hash given by the issuer.

The below image describes how the cert-tools such as cert-wallet, cert-display are used during a transaction. The symbol on the right most certificate would stand for the certificate with the digest or the hash. The below image demonstrates how the recipient requests for the issue of a certificate and the issuer encrypts with the blockchain hash. One of more thing to note here is that the digest is computed based on the contents of the certificate which makes it more authentic and verifiable.

2.4 Challenges

Any application under development faces challenges and always looks forward to overcome those impediments. The challenges face by this application is listed below:

- **Investment for decentralised ledgers**.: Cost of individual ledger is high and use of multiple ones require high capital investment.

- **More maintenance and synchronization between decentralised ledgers:** The whole process is actually split up into multiple ledgers. So ensure the proper functioning of these ledgers, lots of maintenance is required.

- **Computation for decryption adds weight to the processing:** The decryption algorithms used are of certain complexity for security reasons. But this complexity gets added up to the weight of the overall processing.

- **Decentralized ledgers would also mean increase in the network size:** The network size in centralized networks are smaller due to one central server being present. In this architecture, that is not the case as it spreads wide across the place.

- **Complexity is greater compared to centralized systems:** Centralized system required very less computation for its functioning. But in this type of application, computation increases significantly because various computations such as hash digests and decryption

- **Immutability can be a hindrance during updating of information:** If any information regarding a student needs to be updated in the certificate, then it poses an issue as block chains are immutable.

- **Transaction cost can be relatively high compared to existing system:** To perform one transaction the cost is high because of the above mentioned reasons.

- **Network Speed is also affected because of higher computation in the network:** As computation increases the network speed reduces. This is a general trade-off in this type of architecture

- **Scalability:** Scalability is one of the main concerns of any blockchain application but there are alternatives which are being created to enable this feature.

CHAPTER 3

CHAPTER 3

Technology behind the application.

In any application, there are set of protocols that are followed. For instance, in DBMS can have a RDBMS protocol, which works on relationship between two or more entities. Similarly, in a web application, it would be based on SMTP, HTTP, FTP and so on.

Blockchain applications are based on a newly developed protocol which is known as IPFS. IPFS stands for InterPlanetary File Systems.
IPFS (the InterPlanetary File System) is a new hypermedia distribution protocol, addressed by content and identities. IPFS enables the creation of completely distributed applications. It aims to make the web faster, safer, and more open.

3.1 IPFS

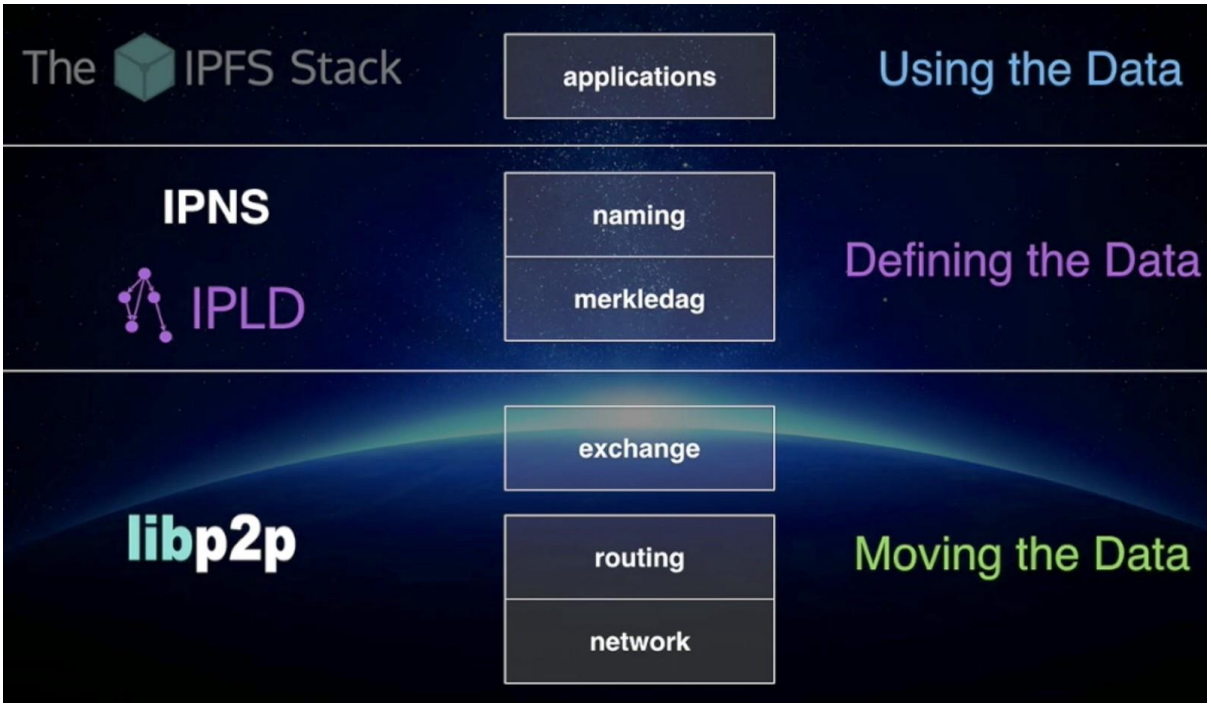

Fig. 3.1 IPFS File System structure

IPFS is combination of few properties, which is stated below:

3.1.1 DHT (Distributed Hash Table)

DHT is a class of a decentralized distributed system that provides a lookup service similar to a hash table: (*key*, *value*) pairs are stored in a DHT, and any participating node can efficiently retrieve the value associated with a given key. Responsibility for maintaining the mapping from keys to values is distributed among the nodes, in such a way that a change in the set of participants causes a minimal amount of disruption. This allows a DHT to scale to extremely large numbers of nodes and to handle continual node arrivals, departures, and failures.

3.1.2 Block Exchanges - BitTorrent

BitTorrent is a widely successful peer-to-peer file sharing system, which succeeds in coordinating networks of un-trusting peers (swarms) to cooperate in distributing pieces of files to each other. Key features from BitTorrent and its ecosystem that inform IPFS design include:

1. BitTorrent's data exchange protocol uses a quasi-tit-for-tat strategy that rewards nodes who contribute to each other, and punishes nodes who only leech others' resources.

2. BitTorrent peers track the availability of file pieces, prioritizing sending rarest pieces first. This takes load off seeds, making non-seed peers capable of trading with each other.

3. BitTorrent's standard tit-for-tat is vulnerable to some exploitative bandwidth sharing strategies. PropShare is a different peer bandwidth allocation strategy that better resists exploitative strategies, and improves the performance of swarms.

3.1.3 Version Control Systems - Git

Version Control Systems provide facilities to model files changing over time and distribute different versions efficiently.
The popular version control system Git provides a powerful Merkle DAG 2 object model that captures changes to a file system tree in a distributed-friendly way.

1. Immutable objects represent Files (blob), Directories (tree), and Changes (commit).

2. Objects are content-addressed, by the cryptographic hash of their contents.

3. Links to other objects are embedded, forming a Merkle DAG. This provides many useful integrity and workflow properties.

4. Most versioning metadata (branches, tags, etc.) are simply pointer references, and thus inexpensive to create and update.

5. Version changes only update references or add objects.

6. Distributing version changes to other users is simply transferring objects and updating remote references.

3.1.4 Self-Certified File systems - SFS

SFS proposed compelling implementations of both (a) distributed trust chains, and (b) egalitarian shared global namespaces. SFS introduced a technique for building Self-Certified File systems: addressing remote file systems.

Thus, the name of an SFS file system certifies its server.

The user can verify the public key ordered by the server, negotiate a shared secret, and secure all traffic. All SFS instances share a global namespace where name allocation is cryptographic, not gated by any centralized body.

Another important concept behind this application would be the use of Merkle trees. This provides the most important aspect of the application which is discussed below.

Merkle tree is a tree in which every leaf node is labelled with a data block and every non-leaf node is labelled with the cryptographic hash of the labels of its child nodes. Hash trees allow efficient and secure verification of the contents of large data structures. Hash trees are a generalization of hash lists and hash chains.
Demonstrating that a leaf node is a part of a given binary hash tree requires computing a number of hashes proportional to the logarithm of the number of leaf nodes of the tree: this contrasts with hash lists, where the number is proportional to the number of leaf nodes itself.

The reason behind the use of Merkle trees:

1. Merkle trees provide a means of proving that integrity / validity of your data.
2. Merkle trees require little memory / disk space and proofs are computationally easy and fast.
3. Merkle tree proofs and management requires only a very small and terse amount of information to be transmitted across a network.
4. Data Existence Verification with Merkle trees:

Let's say you are the owner of the record "2" in the below diagram. You also have, from a trusted authority, the root hash, which in our simulation is "01234567". You ask the server to prove to you that your record "2" is in the tree. What the server returns to you are the hashes "3", "01", "4567" as illustrated in Fig.3.2:

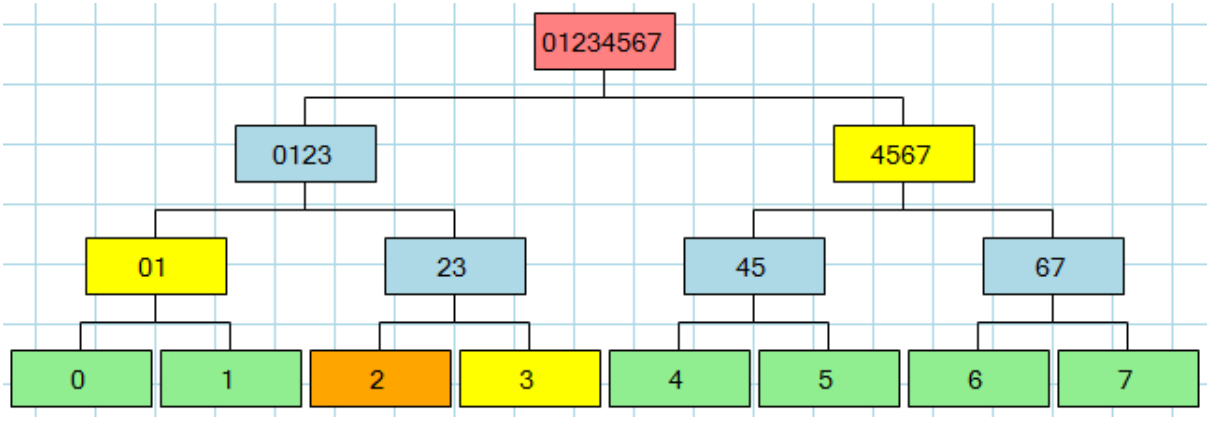

Fig.3.2 Illustration of Merkle Tree

Using this information (including the right-left flags that are sent back along with the hashes), the proof is that:

- 2 + 3 from which you compute 23
- 01 + 23 from which you compute 0123
- 0123 + 4567 from which you compute 01234567

Since you know the root hash from your trusted authority, the proof validates that "2" exists in the tree. Furthermore, the system from which you have obtained the proof is proving to you that it is an "authority" because it is able to provide valid hashes so that you can get from "2" to your known root hash "01234567." Any system pretending to validate your request would not be able to provide you with the intermediate hashes since you're not giving the system the root hash, you're just telling it to give you the proof - it can't invent the proof because it doesn't know your root hash -- only you know that.

In order to verify the proof, very little information about the tree is revealed to you. Furthermore, the data packet that is needed for this proof is very small, making it efficient to send over a network and to make the proof computation.

3.2 Ethereum

Ethereum is an open blockchain platform that lets anyone build and use decentralized applications that run on blockchain technology. In late 2013, Ethereum's inventor Vitalik Buterin proposed that a single blockchain with the capability to be reprogrammed to perform any arbitrarily complex computation could subsume these many other projects. Ethereum is a programmable blockchain. Rather than give users a set of pre-defined operations (e.g. bit coin transactions), Ethereum allows users to create their own operations of any complexity they wish. In this way, it serves as a platform for many different types of decentralized blockchain applications, including but not limited to cryptocurrencies.

Ethereum in the narrow sense refers to a suite of protocols that define a platform for decentralised applications. At the heart of it is the Ethereum Virtual Machine ("EVM"), which can execute code of arbitrary algorithmic complexity. In computer science terms, Ethereum is "Turing complete". Developers can create applications that run on the EVM using friendly programming languages modelled on existing languages like JavaScript and Python.

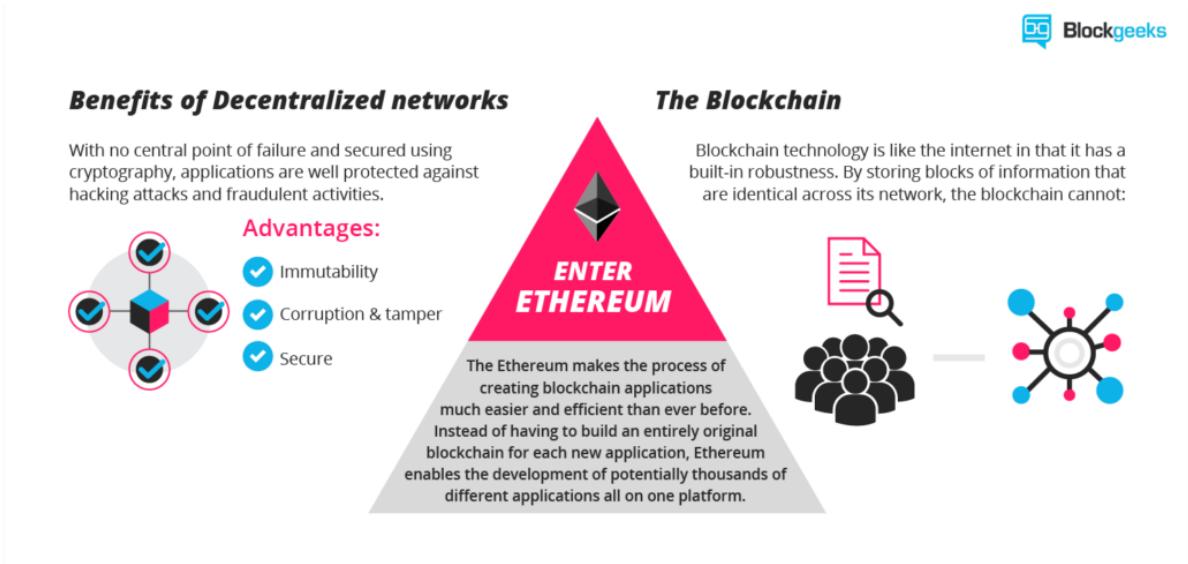

Fig.3.3 Ethereum overview

Like any blockchain, Ethereum also includes a peer-to-peer network protocol. The Ethereum blockchain database is maintained and updated by many nodes connected to the network. Each and every node of the network runs the EVM and executes the same instructions. For this reason, Ethereum is sometimes described evocatively as a "world computer".

This massive parallelisation of computing across the entire Ethereum network is not done to make computation more efficient. In fact, this process makes computation on Ethereum far slower and more expensive than on a traditional “computer”. Rather, every Ethereum node runs the EVM in order to maintain consensus across the blockchain. Decentralized consensus gives Ethereum extreme levels of fault tolerance, ensures zero downtime, and makes data stored on the blockchain forever unchangeable and censorship-resistant.

Ethereum platform satisfies the needs of the project providing robustness and unadulterated verification to ensure the integrity and security of the data.
From a practical standpoint, the EVM can be thought of as a large decentralized computer containing millions of objects, called "accounts", which have the ability to maintain an internal database, execute code and talk to each other.
There are two types of accounts:
1. Externally owned account (EOAs): an account controlled by a private key, and if you own the private key associated with the EOA you have the ability to send ether and messages from it.
2. Contract: an account that has its own code, and is controlled by code.
The code has the ability to read/write to its own internal storage (a database mapping 32-byte keys to 32-byte values), read the storage of the received message, and send messages to other contracts, triggering their execution in turn. Once execution stops, and all sub-executions triggered by a message sent by a contract stop (this all happens in a deterministic and synchronous order, i.e. a sub-call completes fully before the parent call goes any further), the execution environment halts once again, until woken by the next transaction.
Contracts generally serve four purposes:
1. Maintain a data store representing something which is useful to either other contracts or to the outside world; one example of this is a contract that simulates a currency, and another is a contract that records membership in a particular organization.
2. Serve as a sort of externally owned account with a more complicated access policy; this is called a "forwarding contract" and typically involves simply resending incoming messages to some desired destination only if certain conditions are met; for example, one can have a forwarding contract that waits until two out of a given three private keys have

confirmed a particular message before resending it (i.e. multisig). More complex forwarding contracts have different conditions based on the nature of the message sent; the simplest use case for this functionality is a withdrawal limit that is overridable via some more complicated access procedure.

3. Manage an ongoing contract or relationship between multiple users. Examples of this include a financial contract, an escrow with some particular set of mediators, or some kind of insurance. One can also have an open contract that one party leaves open for any other party to engage with at any time; one example of this is a contract that automatically pays a bounty to whoever submits a valid solution to some mathematical problem, or proves that it is providing some computational resource.

4. Provide functions to other contracts; essentially serving as a software library.

Contracts interact with each other through an activity that is alternately called either "calling" or "sending messages". A "message" is an object containing some quantity of ether (a special internal currency used in Ethereum with the primary purpose of paying transaction fees), a byte-array of data of any size, the addresses of a sender and a recipient. When a contract receives a message, it has the option of returning some data, which the original sender of the message can then immediately use. In this way, sending a message is exactly like calling a function.

The first use satisfies the requirement of the project which states the records of the membership of a person in an organization which is similar to the verifying an existence of a person in an institution.

CHAPTER 4

CHAPTER 4

Conclusion

Blockchain is a technology that clearly has applications in the world of learning at the individual, institutional, group, national and international levels. It is relevant in all sorts of contexts: schools, colleges, universities, MOOCs, CPD, corporate, apprenticeships, and knowledge bases.

Rather than the old hierarchical structures, the technology becomes the focus, with trust migrating towards the technology, not the institutions. It is really being a disintermediation technology.

Traditionally institutions have been a source of trust: universities, for example, are trusted "brands". In finance, where blockchain is nowadays a ubiquitous hot topic, banks exist to enact transactions, creating an environment in which blockchain's advantages are readily obvious.

In education, however, there needs to be trust beyond the technology. We are looking, I think, at a hybrid model rather than a wholesale blockchain takeover. Reputation will still matter, and this will continue to be derived from the quality of the instruction, teachers, research, and so on. However, blockchain can play a role here, too, as one could imagine a sort of web of teachers and learners that deploys blockchain to cut out institutions. This, in my view, is not impossible, but it is unlikely.

It must also be recognized and conceded that blockchain is not without its problems. There are data-regulation issues, and a cloud has been created over the technology by the fact that one of the exchanges in the Bitcoin system – which is based on blockchain – saw $500 million disappear. And last but certainly not least, after considerable difficulty, US authorities were able to close down the infamous "Silk Road" drug-dealing exchange, which was also blockchain based.

Yet the biggest obstacle to blockchain's more widespread use is cultural. Education is a slow learner and a very slow adopter. Despite its obvious advantages, the learning world is likely to be slow in implementing this technology, as most of the funding and culture is centered around the individual institution. Bologna was dead the day it was signed as nobody really wanted to lose their students and suffer financially, but it nonetheless became the framework for European higher education. This indicates clearly that the stimulus for change will have to come from elsewhere.

Despite the known issues and compromises from using Blockchain technology for certification, the technology is still in its development. As more researches advance, the technology can be optimized and be more widespread than it already is. Until it tackles sensitive issues, it can be used to solve some general and domestic problems.

REFERENCES

- Using Blockchain Technology to Prove Existence of a Document https://bravenewcoin.com/news/using-blockchain-technology-to-prove-existence-of-a-document/
- Malta Pilots Blockchain-Based Academic Certificate Recording System https://cointelegraph.com/news/malta-pilots-blockchain-based-academic-certificate-recording-system
- Sapiens http://sapiensproject.io/
- Blockcerts - The Open Initiative for Blockchain Certificates https://www.blockcerts.org/
- Using the blockchain as a digital signature scheme https://blog.signatura.co/using-the-blockchain-as-a-digital-signature-scheme-f584278ae826
- IPFS P2P File System, Juan Benet https://securityintelligence.com/why-blockchain-as-a-service-should-be-on-your-radar/
- Blockgeeks https://www.blockgeeks.com/
- Blockcerts Community https://www.community.blockcerts.org