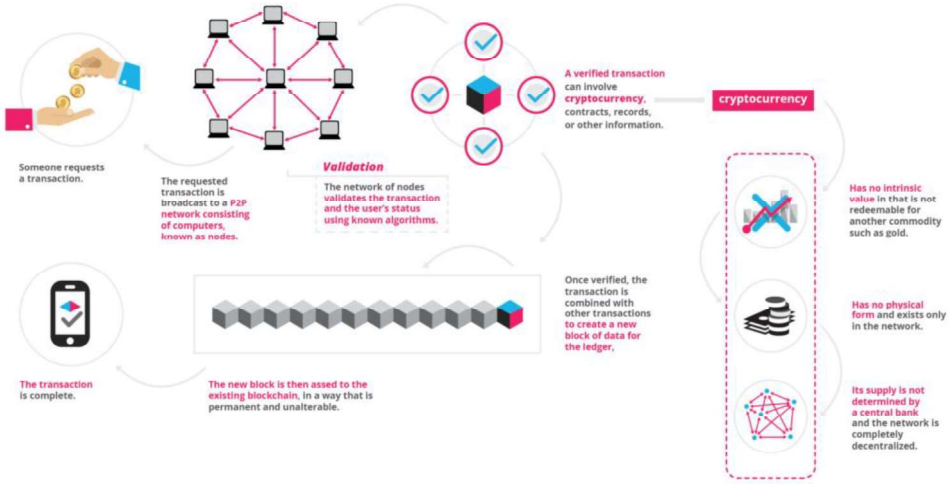

Fig. 1.1 Blockchain working.

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.

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

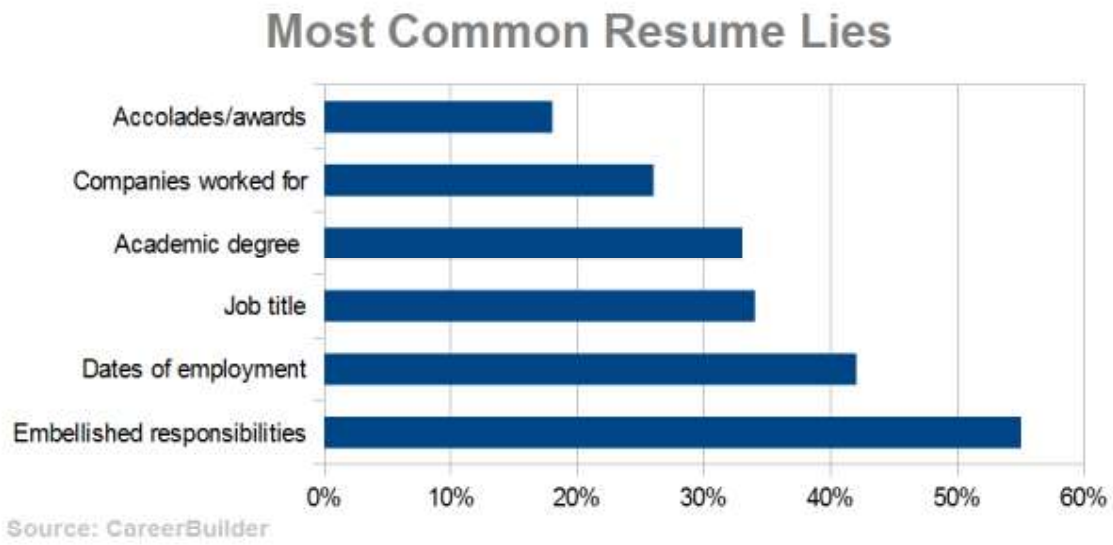

Fig. 1.2 Statistics of lies in Resume.

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:**

2.2 Architecture

2.2.1 System Architecture

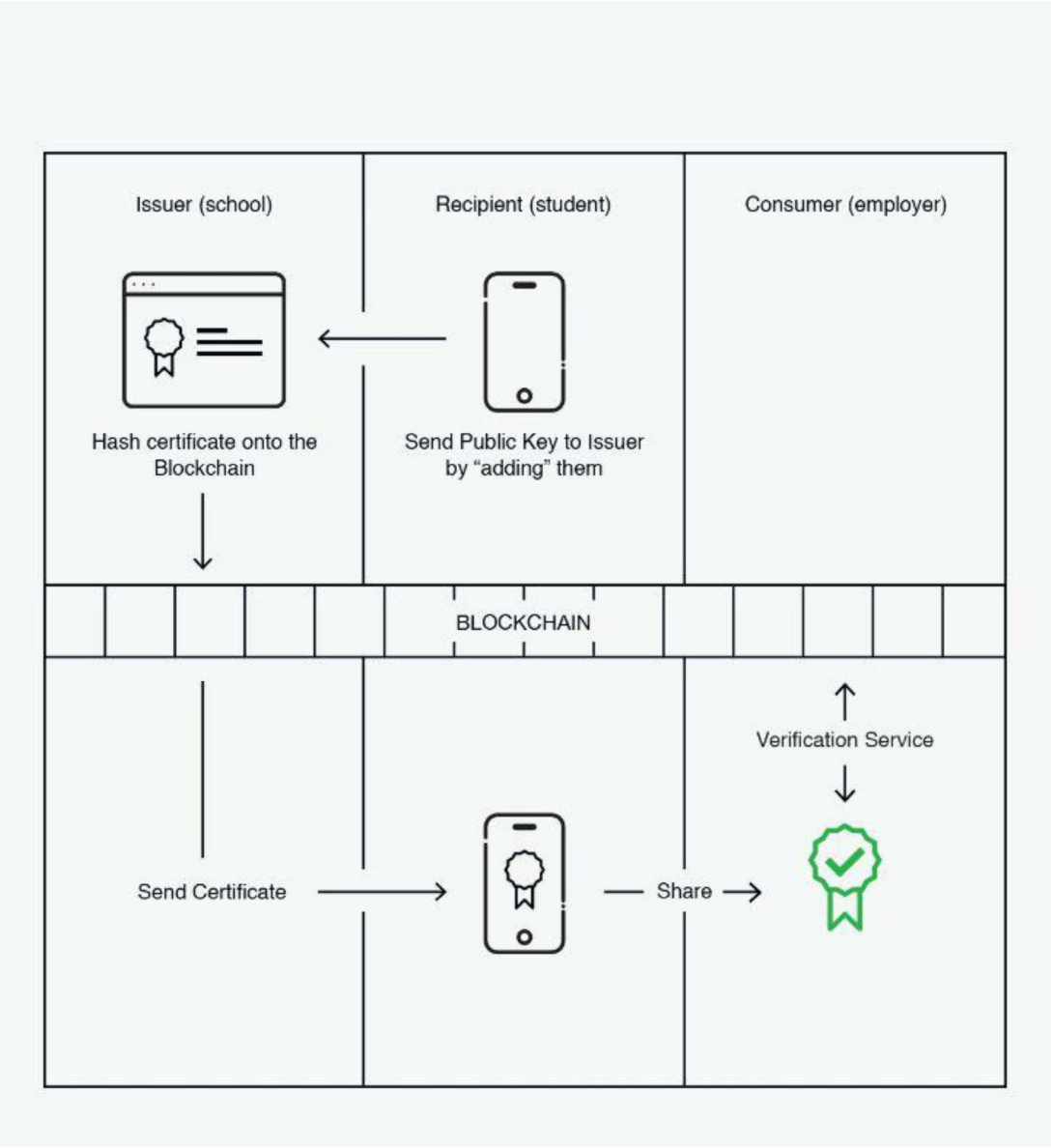

Fig.2.1 Architecture of proposed system

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.

2.3 Methodology

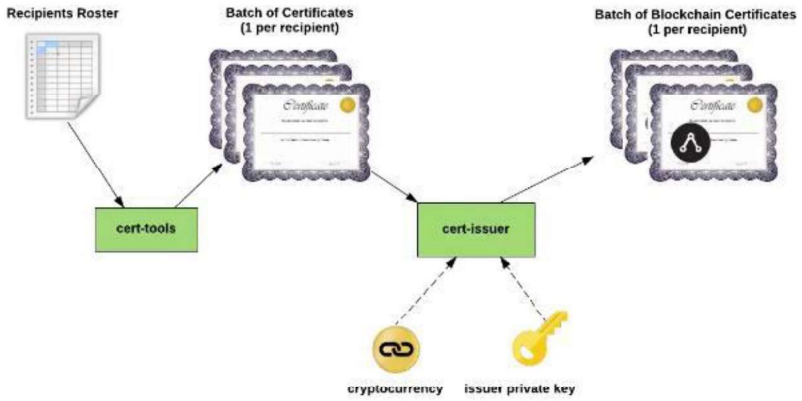

Fig.2.2 Workflow of Proposed system

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.

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

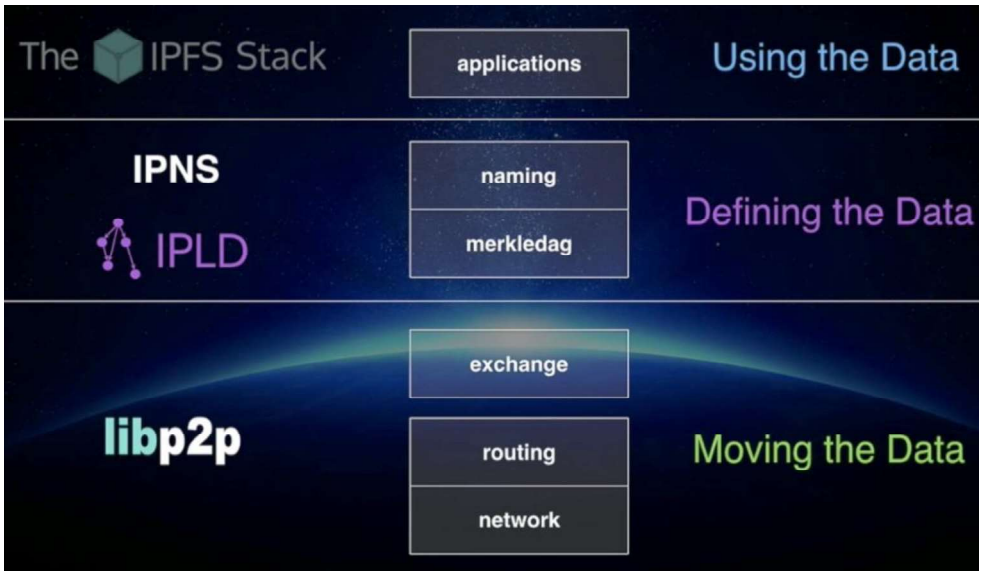

Fig. 3.1 IPFS File System structure

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

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:

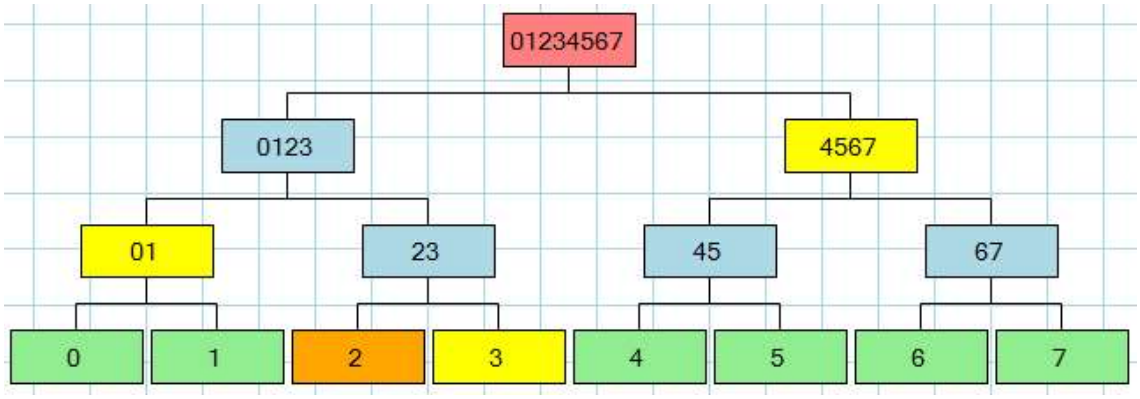

Fig.3.2 Illustration of Merkle Tree

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

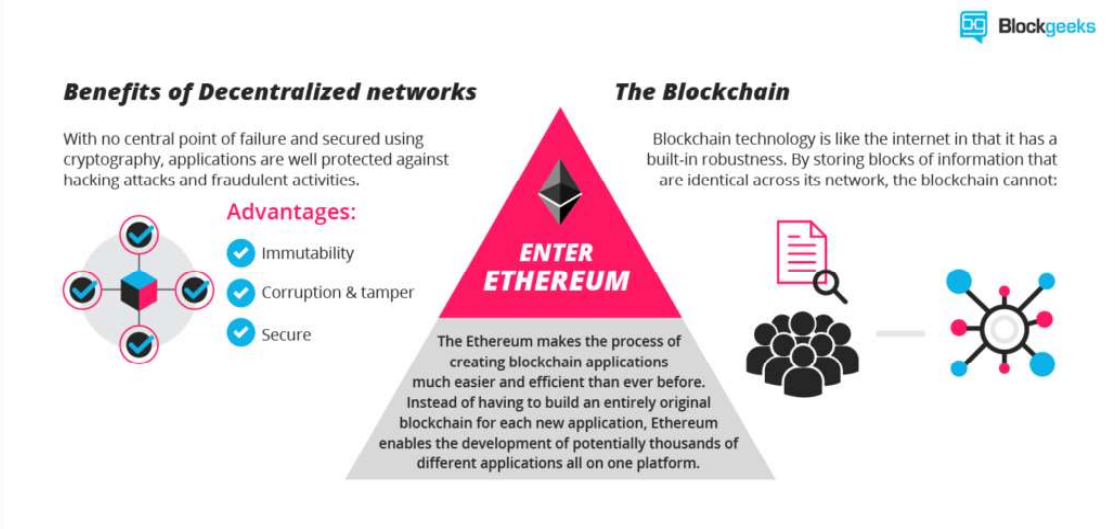

Fig.3.3 Ethereum overview

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.