ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 9, Issue 2, February 2020

Digital Degrees and Markcards Using Blockchain Technology

Neha Sarganachari [1], Kavya S [2], Neeraja [3], Alfia Anjum [4], Sharon Christa IL [5]

U.G. Student, Department of Information Science and Engineering, Dayananda Sagar College of Engineering, Kumaraswamy Layout, Bengaluru, Karnataka, India[1,2,3,4]

Assistant Professor, Department of Information Science and Engineering, Dayananda Sagar College of Engineering, Kumaraswamy Layout, Bengaluru, Karnataka, India[5]

ABSTRACT: The certificates and markcards are very important document for any individual because they serve as a proof of an identity which is required for pursuing their higher studies and job application. Obtaining such an important document via the traditional paper based certificate system is very time-consuming and expensive. The digital certificate is a digital document that is used to prove authenticity and is created by trusted authority. Advancement is technology has enabled the trend of generating fake markcards and degree certificates. Lack of anti-forge mechanism has enabled the forgery and falsification of documents to go unnoticed. Digital Signatures are used in e-documents to provide authentication, integration and non-repudiation but when the key itself is compromised then forgery may happen. Hence, blockchain technology is used to end the incidence of certificate forgeries and ensure security, validity and confidentiality of graduation certificates. Blockchain provides verification of degree certificates within a short period of time and ensures accuracy and reliability of information.

KEYWORDS: Blockchain Technology; Digital Certificates; Graduation Certificates; Digital Markcards; Degree Certificates; Verification; Certificates Forgery; Blockchain for education; Hyperledger fabric.

I. INTRODUCTION

Universities issue certificates to the graduates as a proof of graduate's qualification when they successfully complete the opted course. These marksheets and degree certificates are the important documents required to apply for jobs and further studies. A graduation certificate is mostly in the form of a paper-based document as an electronic document cannot effectively replace a physical certificate [1]. The document validation and verification have become important tasks. It is necessary to validate that the graduation certificate presented by the graduate is genuine and the owner is the rightful owner with proper authorization. The traditional paper-based certificates are time-consuming and costly. They are even vulnerable with fraud occurring through forgery and mistakes. Paper based mark sheets are inaccessible, limited flexibility, lengthy process and non eco-friendly. However, due to the presence of advanced and cheap technologies, the forgery of certificates has increased. This threatens the integrity of the certificate holder and the university that issued the certificate [2]. This paper proposes a solution wherein the generation of degree certificates and verification of the same is digitalized using blockchain technology. The immutable property of blockchain ensures that the markcards are free from forgery and falsification.

II. PROBLEM STATEMENT

The traditional paper based degrees and mark cards are vulnerable with fraud occurring through forgery and mistakes. Paper based markcards 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 markcards

ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 9, Issue 2, February 2020

validation as fake markcards and degree certificates are rampant everywhere. . So this paper intends to propose a system that eliminates the forgery of certificates.

III. LITERATURE SURVEY REVIEW

1. The new Blockchain based system reduces the certificate forgery and ensures authentication, integration and security.
2. Students demand a proof-of-certification at low cost and easy to check, employers also demand quick and trustable verification of degrees when recruiting [3].
3. Digital certificates are registered on the Bitcoin blockchain, Cryptographycally 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 [4].
4. The blockchain's hash function offers a better strategy for signature preservation. Blockchain adoption is more advantageous to records with a permanent retention schedule [5].

IV. RELATED WORK

The traditional paper based certificate system depends upon third party system for transfer and validation of academic records which makes them time consuming and economically infeasible. The digital certificates are also prone to forgery if the key itself is compromised. The certificates issued to the students are mostly in the form of paper. The paper based marksheets are inaccessible. During this process, much time will be spent either in 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 especially if a company needs to check the certificates of several hundreds of applicant [6]. The physical mark sheets or certificates may be damaged or lost due to negligence of the certificate holder or due to some other reasons. In such cases, the duplicate or copy of certificates cannot be retrieved immediately as it is a lengthy process and this limits the flexibility of the certificates . The paper based certificates are non eco-friendly because paper requirement is satisfied from cutting down of woods in the forest area. Dependency on third-party verification agencies to contact issuing authority and verify the documents authenticity. A fee is charged for each verified document [7]. Due to advancement in information technology and lack of anti-forge mechanisms available, the forgery and falsification of the degree markcards and certificates goes unnoticed.

In the digital certificate system the concept of cryptography is used. In public key cryptography, if the key itself is compromised then the forgery of the certificate is expected. Since the certificate authorities are the ones in charge of issuing digital certificates, hackers often target these authorities to manipulate the certificates and other documents. The existing project such as MIT Digital Certificates Project [8] provides a system for registering the digital certificates to the Bitcoin blockchain, which can then be shared and verified. This is permissionless blockchain application. Bitcoin blockchain include long transaction times, and the solution may not be scalable to a larger number of requests that would be required for adoption to larger academic institutions. Other solutions using permissioned blockchains include CredenceLedger [9] which operates on a permissioned blockchain using multichain streams. It records hashes of the records within the blockchain, with a mobile application front end interface for students to manage their credentials [10].

V. BLOCKCHAIN TECHNOLOGY

The concept of blockchain was first proposed by a person named Satoshi Nakamoto in 2008. Blockchain is an emerging technology and has lots of application in various fields. Blockchain technology with its remarkable features and characteristics is used in cryptocurrencies, infrastructure, agriculture, educational domain, health care domain, banking solutions and so on. This paper is about use of blockchain technology in educational domain. Blockchain is basically a Distributed Ledger Technology that allows all members to record transactions in a decentralized data log

ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 9, Issue 2, February 2020

maintained on a network of computers rather than a physical ledger or a single databases. Transactions are approved by consensus, and everything is secured through cryptography. Blockchain application in various domains is now being promoted actively by the government. 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 centralized control among individual nodes, based on such techniques as data encryption, time-stamping, distributed consensus algorithms, and economic incentive mechanism [11].

This section discusses about the blockchain features. The blockchain features are truly making changes and are useful because of less failure, user control, less prone to breakdown, no third-party, zero scams, transparency, authentic nature. The immutability is one of the key feature in blockchain technology. The data of multiple transactions are stored in the form of block along with timestamp, 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 (immutable property) which helps in preventing forgery [12]. 101 Blockchains by Hasib Anwar gives the following important blockchain features:

1. **Cannot be Corrupted:** Every node on the network has a copy of the digital ledger. To add a transaction every node needs to check its validity. If the majority thinks its valid, then its added to the ledger. This promotes transparency and makes it corruption-proof.
2. **Decentralized Technology:** The network is decentralized meaning it doesn't have any governing authority or a single person looking after the framework. Instead, a group of nodes maintain the network making it decentralized.
3. **Enhanced Security:** As it eliminates the need for central authority, no one can just simply change any characteristics of the network for their benefit. Also using encryption ensures another layer of security for the system.
4. **Distributed Ledgers:** The ledger on the network is maintained by all other users on the system. This distributes the computational power across the computers to ensure a better outcome.
5. **Consensus:** Every blockchain thrives because of the consensus algorithm. The architecture is cleverly designed, and consensus algorithms are at the core of its architecture. Every blockchain has a consensus to help network make decisions.
6. **Faster Settlement:** Blockchain offers a faster settlement compared to traditional banking systems. This way a user can transfer money relatively faster which saves a lot of money in the long run.

A. BLOCKCHAIN FOR DOCUMENT VERIFICATION

The blockchain finds one of its applicability in document verification processes. A digital certificate in a light of blockchain technology could address the forgery and falsification issue. The documents to be verified are set on a distributed ledger. It is not the digital copy rather a cryptographic copy that is stored on the blockchain network. Suppose University has decided to store every degree certificates on blockchain technology. The first step of precedence will be the converting document content to one way hash code using cryptography. The hash code is further stored inside the blockchain. The one-way hash code resembles the copy of the document but represented as a string of codes. This strings of codes act as a key for the document. When the user presents this document elsewhere, the code remains same as stored in the blockchain. When recruiter is in need of hiring a graduate and he requests for certificate verification, the former can authenticate certificate via just hashing the content to a cryptographic mode. If the hash matches the details stored on blockchain by the university, the degree certificates produced are genuine. If the documents are altered, it will not match. The article in Medium.com gives the following details.

ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 9, Issue 2, February 2020

1. Document verification on blockchain technology eliminates the third party thus limiting the cost of transaction on the network.
2. Certificates are placed on a distributed ledger so that people can have access to information anytime, anywhere. Under blockchain, the documents are securely placed that only authorized person can access using their private keys.
3. Blockchain stores data in a form that cannot be altered. This is done through cryptography which involves encryption of data using a hash function. So data becomes unalterable.
4. There will be no scalability issue anymore as transaction time taken could be as quick as few seconds. In this manner, Documents verified on blockchain allows quick delivery of service.

VI. METHODOLOGY FOR PROPOSED MODEL

To eradicate forgery and falsification of certificates , this paper proposes a permissioned blockchain based solution. Blockchain are of two types: permissioned and permission-less blockchain. Under permission-less blockchain, Ethereum framework is used to build application that reduces transaction cost and expands functionality. Under permissioned blockchain, Hyperledger fabric is used. To achieve digital degrees and markcards using blockchain technology, we are using Hyperledger fabric which is a modular blockchain framework and acts as a foundation for developing blockchain based products, solutions and applications using plug and play components.

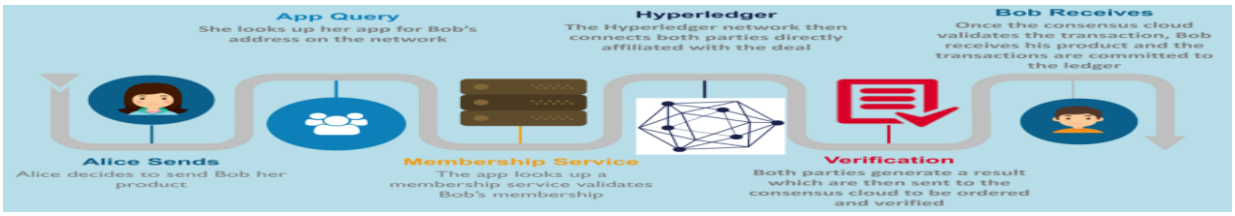

Fig 1. Hyperledger Workflow. Source: "What is Hyperledger|Introduction to Hyperledger Project" by Edureka.

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, B receives his document and the transactions are committed to the ledger.

A. SYSTEM ARCHITECTURE

In this proposed model, the application architecture has three main components-front end web application, Interplanetary file system (IPFS) and Hyperledger fabric as our backend.

ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 9, Issue 2, February 2020

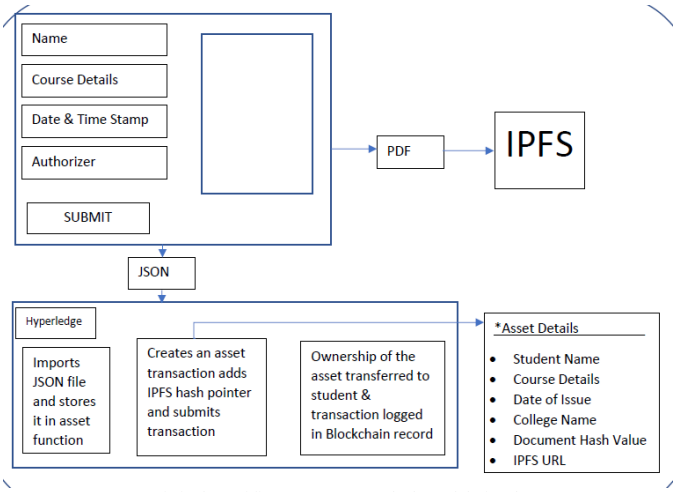

Fig 2. Application Architecture. Source: "Digital certificates on Hyperledger fabric" by Apurv.S at medium.com, Aug.20,2018.

We cannot store images in blockchain, so to overcome this we are integrating our system with IPFS. IPFS is a peer to peer method of storing and sharing media in a distributed file system. The student details such as name, USN, college name etc are added on the web applications. The web application then generates a digital certificate in PDF and JSON formats. The PDF is a copy that is uploaded to IPFS node and the hash pointer is saved. The JSON file is imported by hyperledger to create an asset, the hash pointer link is also added to the digital certificate. Once such digital certificate is created by the institution and issued to the student, the student can then send copies of this digital asset to the several beneficiaries without any added cost to the university or the student. We can manage the access levels as it is hosted on Hyperledger blockchain. And one who receives the digital certificate as the proof of credentials will have a clear view of the history of the certificate. The certificate will contain the immutable record of the issuing authority, date, time of issuance and the owner of the certificate. When a valid user requests for a certificate, the requested certificate is uploaded to the web server and the hash code is generated. The certificate and a hash code are sent to the user via email or downloaded on the user machine and the hash code is stored in the blockchain repository. The verifier can compare the hash given to the user with the hash stored inside blockchain. If both the hash value matches then the certificate submitted by the user is valid otherwise it is modified and invalid.

B. HARDWARE AND SOFTWARE REQUIREMENTS

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

HARDWARE REQUIREMENTS:

Processor – Intel® Core™ i8
RAM - 4.00GB / 8.00GB
Hard drive - 1TB

SOFTWARE REQUIREMENTS:

Operating system - Ubuntu Linux 14.04 / 16.04 LTS (both 64Bit) or Mac OS 10.12
Framework - Hyperledger Fabric
Tools - Hyperledger Composer

ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 9, Issue 2, February 2020

Docker engine - version 17.03 or higher
Docker Composer - version 1.8 or higher
Code Editor- Visual Studio Code
Programming language- python 2.7 or Go or Java.

C. USE CASE DIAGRAM

1. The admin will login to the system and can view and update his profile details. He has a privilege to view and modify the server details and owner details with options add, edit and even delete them.
2. The owners can login to the system and can view and update their profile details. The owners can view the user requests and upon validating the user they can upload the requested file. The owners are having a privilege to provide access control to the various users. The transaction is recorded.
3. The user has to register first and then login to the system where he can update his profile details. He requests for a secret key to download his file. If he is a valid user then he can download a file with the requested secret key otherwise the access is denied.

Fig 7. Use case diagram for Admin (a), Use case diagram for Owners (b), Use case diagram for Users (c).

ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 9, Issue 2, February 2020

D. SEQUENCE DIAGRAM

The following sequence diagram includes all the steps in sequential order from requesting certificate by the user to the downloading of requested certificate. The admin is the one who is able to validate, add, edit and delete the owners, domains and sub-domains to the system. The admin provides each owner a publisher key which is used by the owners to login to the system. The admin has the privilege to access server and do required settings. The owners are the one who are responsible for validating the user request and issuing the certificate to the valid user. The users are one who is in need of graduation or degree certificates. The process of getting the blockchain based certificate involves the following steps:

1. The *admin* is having the privilege of doing proxy server settings. The admin has the owner/publisher details. The owners are provided with the publisher key and each time they login to the system the admin needs the confirmation of the valid owner. The admin also keeps track of domain and sub domain details.
2. The valid *owners* can view the user request and once the owner validates the user details he can generate a secret key for requested user. The owner upon confirmation, uploads the requested file.
3. The *users* has to first register themselves before making a request. After registration if the user is a valid person then he will be provided with the identity token key using which the user is able to login to the system. After logging in the users requests for secret key which is generated by the owner for particular user, using which he can request for certificate or file to download. If the user is valid user then he can download the file otherwise the access is denied.

Fig 7. Sequence diagram for the proposed project.

E. MODULE FLOW DIAGRAM

A modular design reduces complexity of the system, facilities changes,which results in easier implementation by encouraging parallel development of different part of the system [13]. The module flow diagram has five important modules as shown in the figure below. These following modules are integrated to satisfy the requirements of the proposed project. The modules are as follows:

1. User Interface Design
2. Server

ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 9, Issue 2, February 2020

3. Blockchain
4. Verification

The user interface design module comprise of the front end web application that allows the students and universities to register through simple form filling. The universities and students database is updated every time a user register. The student belonging to particular university is eligible to request certificate only from that university. If the user is a valid student then the university uploads the requested document to the web server and computes the hash of the certificate. The student can now download his certificate. The valid transactions are committed to the blockchain i.e. the hash of the certificate is stored in the blockchain rather storing an entire file. The potential employees and other universities can now run the same hash function on the certificate provided by the student and compare the hash generated with the hash present in blockchain for that particular certificate. If both the hashes are same then the markscard is valid otherwise it is invalid.

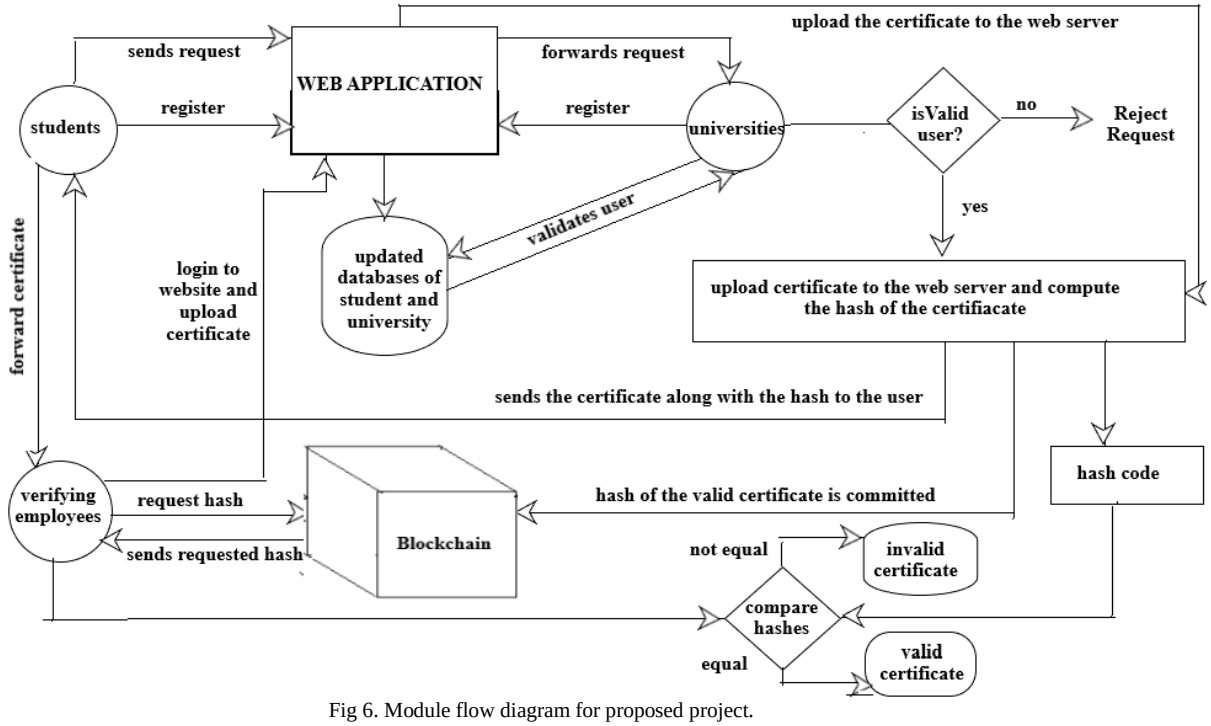

Fig 6. Module flow diagram for proposed project.

VII. CONCLUSION

The immutable property of blockchain technology prevents alteration of any record which is placed in the blockchain repository. It provides authentication, integration and security. Digital degree certificates are made available online which saves time and reduce cost. In case of loss or damage of original markcards or certificates, the copy of originals can be obtained through online hence provides lot of flexibility. The documents stored in the blockchain repository can neither be altered nor be deleted hence provides security. The universities, students and recruiters are the main beneficiaries of this system because it ease the process of generation and verification of certificates and markcards. In conclusion the proposed model eliminates the forgery and falsification of certificates and recruiters can be sure of getting reliable information from blockchain repository.

ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 9, Issue 2, February 2020

REFERENCES

[1] M. Warasart and P. Kuacharoen, "Paper-based Document Authenticating using Digital Signature and QR Code," no. Iccet, 2012.
[2] Z. Chen, "Anti-Counterfeit Authentication System of Printed Information Based on A Logic Signing Technique."
[3] Oliver,Miquel;Moreno,Joan;Prieto,Gerson;Benitez,David(2018):"Using Blockchain as a tool for tracking and verification of official degrees: business model",29th European Regional Conference of the ITS.
[4] Juliana Nazare,Kim Hamilton Duffy, J. Philipp Schmidt "Digital Certificate Project" MIT Media Labs, 2015.
[5] Stephen Thompson "The Preservation of Digital Signatures on the Blockchain" University of British Columbia iSchool Student Journal ,vol.3 (Spring 2017).
[6] Osman Ghazali and Omar S. Saleh, "A Graduation Certificate Verification Model via Utilization of the Blockchain Technology", *e-ISSN: 2289-8131 vol. 10 no. 3-2.*
[7] X. Technologies, "Blockchain imperative for educational certificates," *Xanbell Technologies, 2017.*
[8] MIT Media Lab Learning Initiative and Learning Machine, "Digital Certificates Projects." [Online]. Available: http://certificates.media.mid.edu/.
[9] R. Arenas and P. Fernadez, "CredenceLedger: A Permissioned Blockchain for Verifiable Academic Credentials." In *IEEE international conference on Engineering,Technology and Innovation (ICE/ITMC*). Stuttgart, Germany 2018.
[10] Ahmed Badr, Laura Rafferty, Quassy H. Mahmoud, Khalid Elgazzar, Patrick C.K. Hung "A Permissioned Blockchain-Based System for Verification of Academic Records" in IEEE 2019.
[11] Neethu Gopal and Vani V Prakash, " Survey on Blockchain Based Digital Certificate System," *IRJET,* vol. 5, Issue: 11 | Nov 2018.
[12] Nitin Kumavat, Swapnil Mengade, Dishant Desai, Jesal Varolia, "Certificate Verification System using Blockchain," *IJRASET vol. 7 Issue IV, Apr 2019*
[13] T. Keerthana, R. Tejaswini, V. Yamini, K. Hemapriya, "Integration of Digital Certificate Blockchain and Overall Behavioural Analysis using QR and Smart Contract*", IJRESM vol. 2, Issue-3, March 2019*