International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-10 Issue-11, September 2021

Decentralization of Credential Verification System using Blockchain

Priti P. Bokariya, Dilip Motwani

Abstract*: After successful completion of graduation, students receive the credits of the courses in the form of certificate issued by the respective University. A Student have to produce his/her documents to the employers or the authorities for employment or higher education. Today ,as the system is centralized all the data resides on the server which can be hacked or the data can be lost if the system crushes down. However, verifying a certificate by authorities, is a time-consuming process as there is an involvement of human resources ,for validating the details of the candidate from its University. Today , with the advancement in technologies and due to the easy availability of many efficient soft wares that have led to the forgery of credentials/certificates. The lack of anti-tampering mechanisms resulted in incidents where the forged graduation certificates are often found. Also ,in case certificates are out of place , applying for duplicate certificates and its issuance by the University consumes a lot of time. Use of blockchain technology in this process will make the system decentralized as blocks as cryptographically connected and all the nodes in the network shares the entire chain .Hence the proposed decentralized certificate verification system, uses blockchain technology incorporating all the essential features in developing a DAPP. This system is proposed to address the issue of certificate counterfeiting, faster certificate verification and issuance. Putting across all the issues, the system aims at addressing the problems and provide solutions to the current Certificate Issuance, verification and Validation Process.

***Keywords* : Blockchain, cryptography, DAPP**

I. INTRODUCTION

Students who have completed their studies receive credits from universities. The credits earned by the students by acquiring the skills in the course are typically in the form of ,a graduation certificate. As the technology has enormously advanced and the easy availability of efficient tools has led to duplication of such certificates. This jeopardizes the legitimacy of the system. This puts the certificate holders' and the university that gave the certificate's reputation in jeopardy. It is important to verify that the graduate's graduation certificate is authentic and that the bearer of the certificate is the authentic owner. Furthermore, it is equally important to validate the contents on the graduation certificates and that it originates from a legitimate source.

Manuscript received on September 20, 2021.
Revised Manuscript received on September 24, 2021.
Manuscript published on September 30, 2021.
* Correspondence Author
Ms. Priti P. Bokariya*, Department of Computer Science and Engineering SVKM's Shri Bhagubhai Mafatlal Polytechnic, Mumbai, India. E-mail id. priti.bokariya@sbmp.ac.in
Dr. Dilip Motwani, Associate Professor Vidyalankar Institute of Technology, Mumbai. India.

Also, the graduates, whether they plan to continue their education or begin looking for work, would need a variety of certificates for job interviews. that: However, they may discover, that their commendation certificates are not in place. Since certificates are issued by various organizations, applying for it again may consume lots of time. In certain cases, an in-person application might be required. Applying for an e-copy, on the other hand, will save both paper and time. Graduates can easily apply for any credential by supplying details for identity verification. Nonetheless, forgeries of degree certificates, licenses, and certificates are common as a result of this convenience. As a result, schools and businesses are unable to immediately verify the documents they obtain. This project leads us with an idea to create a DAPP with appropriate solution. As the underlying technology is Blockchain and the information is stored on all nodes in the network , and to tamper with the internal datum would be not possible .In the traditional system, to confirm the legitimacy of the certificate ,to validate the contents on the document, also to verify all the essentials and the University to respond back on the authenticity of the candidate holding the document is a manual process which takes a lot of time. One benefit of digital systems is that credentials can be quickly verified. Hence the Blockchain domain would be adapted to implement this system. Either Ethereum or Hyperledger platform shall be used for the same. Technologies like REACT, Python, JavaScript with Solidity programming also can be used for developing a DAPP.

II. TRADITIONAL ACCREDITATION SYSTEM

Today, the academic degrees in various fields are awarded by universities. In this sense, a credential is a certified document by the University awarding the degree or diploma to the graduate in lieu of successfully and satisfactorily completing the requirements of an educational program. Hence these certificates qualify the candidate and are produced as a proof of their graduation wherever needed for most opportunities in life. So ,consequently, there is a remarkable need among authorities to ensure that the degree certificate is held by the authentic candidate . All the Universities mostly adapt the same process to issue the certificate to the students accredit it and validate it .Also the employers verify it through the certified documents from the respective Universities Academic certificates provided by educational institutions are checked and validated by accreditation agencies, which are either national or private organizations. Once the credentials are submitted by the prospective students to the employers or authorities to procure a job or higher education, the verification of those certificates takes a lot of time as it is done manually.

Also, as this system is based centrally it can be tampered with. The certificates can be duplicated or a student may, for example, try to counterfeit a credential or buy one from a diploma mill. Fake degrees may be sold by a university. Fake degrees may be accepted by an accreditation body. Malicious parties can also work together. There would be no validation of such duplicate certificates, which is biggest failure of the system. The duplicate certificates would be verified easily by the employers in such a case and the prospective candidate would be hired with its fake degree. Use of decentralized accreditation system would assure the authenticity of certificates.

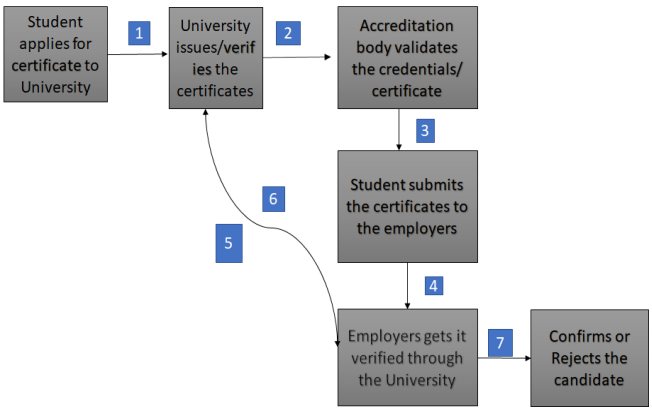

Fig.1

The above Fig 1 depicts the flow of the conventional existing Certificate Verification Process in India which is centralized system and time consuming .

III. LITERATURE SURVEY

[1] INTERNATIONAL JOURNAL OF SCIENTIFIC & TECHNOLOGY RESEARCH VOLUME 9, ISSUE 03, MARCH 2020 ISSN 2277-8616 82 IJSTR©2020 www.ijstr.org Educational Certificate Verification System Using Blockchain Dinesh Kumar K, Senthil P, Manoj Kumar D.S

The verification of documents submitted by prospective employees by the employer is essential before offering jobs. As the process is manual it takes ample amount of time for the candidate to receive an offer letter. The authorities issuing certificates verifies the authenticity of the certificates and acknowledges it to the employers. Such time-consuming verification process delays the hiring process. As a solution to counterfeit the academic certificates a distributed ledger is provided by Blockchain along with the cryptography mechanism. Use of Blockchain makes it possible to have a shared platform for warehousing and retrieving the certificates, hence minimizing the time required for verifying the certificates.

[2] Efficient Certificate Management in Blockchain based Internet of Vehicles Ei Mon Cho 1, Maharage Nisansala Sevwandi Perera22020 20th IEEE/ACM International Symposium on Cluster, Cloud and Internet Computing (CCGRID)

As the Online of Vehicle (IoV) research trend continues, the privacy and security of each internet automobile has become a hot topic. This study aims to lower the cost of securely certifying documents such as graduation certificates. The distribution and maintenance of the Certificate Revocation List (CRL) in vehicle public key infrastructure are addressed in this article using blockchain technology (PKI). For the blockchain mechanism, the suggested scheme employs activation codes to validate the certificate based on time to non-revoked vehicle. We want to cut the cost of certification and, of course, do rid of the certificates for automobiles that are no longer in use.

[3] Design and Implementation of Work Training Certificate Verification Based On Public Blockchain Platform 1st Irawan Afrianto Informatics Engineering Department, 2nd Yayan Heryanto Informatics Engineering Department

The goal of this study is to create a public blockchain-based system for storing job training documents. Certificate data is secured using public platforms, making it harder to forge. Smart contracts are used to create data for blocks that will be delivered to the Ethereum blockchain network. The Inter Planetary File System (IPFS) is used to store certificate files in a distributed environment, allowing for quick and secure access. The findings revealed that certificate data can be kept on the Ethereum public blockchain architecture, with supporting files in the IPFS environment. The findings revealed that certificate data can be kept on the Ethereum public blockchain architecture, with supporting files in th IPFS environment

[4] Efficient Distributed Admission and Revocation using Blockchain for Cooperative ITS Noureddine Lasla∗, Mohamed Younis§, Wassim Znaidi∗ and Dhafer Ben Arbia∗ ∗Qatar Mobility Innovations Center (QMIC), QSTP, Doha, Qatar

The Cooperative Intelligent Transportation System (CITS) allows vehicles to communicate with one another and it alerts that add on to the safety on roads .Also its presumed that this technology is going to hit the market in coming days, but fundamentally the question arises regarding communication security remain a source of research worry. Current inter-vehicle communication security solutions rely mostly on the authentication of digital certificates. Furthermore, as its computation is very expensive and the validation of certificate need to be done within a specific time frame, such a solution imposes significant overhead on vehicles. Furthermore, relying on a central node to decide on certificate issuance and revocation provides a single point of failure and may jeopardise motorist safety. Here it is propose using Blockchain to maintain track of each vehicle's certificate (valid or revoked) in distributed and immutable records in this study. In essence, we use a lightweight blockchain-based authentication solution to replace certificate verification. A fully distributed vehicle admission/revocation method is also proposed. We show that our technique can reduce calculation overhead and improve performance.

[5] Cerberus: A Blockchain-Based Accreditation and Degree Verification System Aamna Tariq∗ , Hina Binte Haq, Syed Taha Ali‡ School of Electrical Engineering and Computer Sciences (SEECS), National University of Sciences and Technology (NUST), Islamabad, Pakistan.

The forgery of certificates is common occurrence which jeopardizes the trust in the higher education system while also causing major economic and social harm. Verification of certificates by the traditional process consume lot of time, expensive, and complex, and they make efforts to combat some types of frauds in certificates. In this work a comprehensive solution that is based on blockchain identity verification is offered that would be significantly more efficient, easier to use, and efficiently mitigates prevalent credential fraud manifestations. This system also outperforms the available solutions in the literature of blockchain, by adhering to a current credit authentication infrastructure and addressing a threat model based on factual theft situations. For credential revocation, there is an employment of on-chain smart contracts, so students and employers don't have to worry about managing digital identities or cryptographic credentials in order to use the system. Here ,this paper presents a prototype of the system and detail the efforts to provide an online verification service with a comprehensive feature set that includes data privacy, transcript verification, and selective data sharing. The system presented in this paper has contributed to alleviate the problem of forged credentials.

IV. RELATED WORK

1.Blockchain:

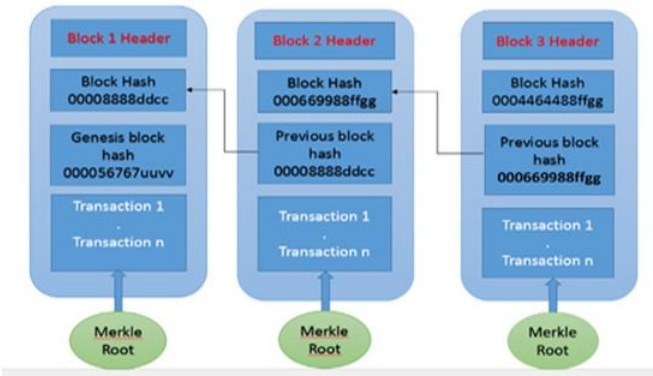

Fig.2

Distributed ledger technology,i.e Blockchain wherein the sharing of data is decentralized. Every block of a blockchain contains set of transactions. The transactions in the block could be cryptocurrency transaction, digital certificate, bill of lading etc., these transactions need to be communicated to all the nodes in the blockchain. The miners validate the transaction and clump them together in a new block .This new mined block will be appended to the distributed ledger. Blocks in the transaction are cryptographically sealed making them tamper proof thus ensuring security. In this technology the database is distributed that stores or records the various transactions. The transaction is added to a block that already contains records of numerous transactions whenever a consensus is obtained among different nodes. For connection, each block carries the hash value of its previous counterpart. The blocks are all linked together, forming a blockchain. The fundamental of Blockchain is to have a distributed ledger that is used to keep track of individual transactions. Different nodes validate each transaction. Accepting legal transaction is finalized using consensus algorithm like permission less consensus algorithm and permissioned consensus algorithm. There are two types of block chain. The first is the Blockchain 1.0 version, which is utilized in applications such as bitcoin and as a public ledger for replicating data. Blockchain 2.0 is a decentralized system that transforms assets using smart contracts, allowing for transaction automation. The basic goal of Blockchain 1.0 is to allow any parties to deal directly with each other in an untrustworthy environment. The signed transaction is irreversible, which protects the parties against fraud, inconsistency in the transaction, and ensures that all parties have access to the same transaction data in the ledger. Every block is cryptographically encrypted in the blockchain, with the current block's transaction details and block header hashed using the double SHA256 technique. The Block header contains the hash of previous block nonce, time stamp, version, Merkle root hash.

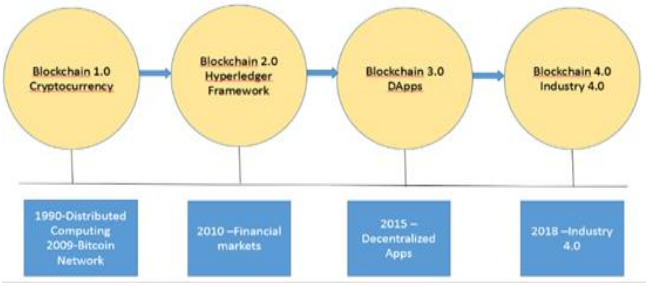

Fig.3

2.Smart Contract

- **Private Smart Contract**

Permissioned blockchains are gaining popular in industry, because they can boost efficiency in a closed network conduct business transaction, a private blockchain with a small number of stakeholders is used. The cost of validation in a public blockchain is extremely high. When compared to permissioned blockchain, the energy spent on the consensus process to do proof of work is significantly high. As a result, private blockchain can be efficient if the number of nodes is small and the efficiency is good if the transactions are faster. The consensus process utilized in public and private blockchains will be different. Proof of work and Proof of Stake are the consensus algorithms used in public blockchain. To develop a blockchain environment for business use. Hyperledger fabrics, Hyperledger composer, Hyperledger Indy, and Hyperledger Sided are IBM's blockchain development environments for business services. Members of the Hyperledger Fabric are permissioned blockchain networks that participate in the development of the Hyperledger Fabric. The network's member organization is in charge of assigning peers to network participants. The certificate authority certifies each peer in the network.

- **Public smart contract**

As permission less blockchain does not require peer nodes to participate, all peer nodes are able to deploy smart contracts. To avoid spamming, participants must pay a small charge when creating and running the programs i.e. smart contracts. Smart contracts are created in public blockchain apps like bitcoin utilizing bitcoin scripts, which are used to create contractual conditions.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication

Ethereum may also be used to control money and develop a variety of decentralized applications. Eth is a cryptocurrency that was created in the Ethereum environment.

- **Ethereum**

An open-source technology, block chain-based, decentralized software platform that was launched in 2015 and is utilized for its own cryptocurrency, ether. It enables Smart Contracts and Distributed Applications (ĐApps) to be built and run without any downtime, fraud, control, or interference from a third party. Ethereum is not just a platform but also a programming language (Turing complete) running on a blockchain, helping developers to build and publish distributed applications.

- **Ethereum Virtual Machine (EVM)**

Ethereum is a blockchain that can be programmed. Instead of providing users with an or before set of operations (such as bitcoin transactions), Ethereum empowers them to design their own operations of unlimited complexity. It provides as a platform for a variety of decentralized blockchain applications, including but not limited to cryptocurrencies, in this fashion .In its most basic form, Ethereum can also be referred to as a set of protocols that facilitates a decentralized application platform. The Ethereum Virtual Machine ("EVM"), which can run code of any algorithmic complexity, lies at the heart of it. Ethereum is "Turing complete" in computer science jargon. Using friendly programming languages modelled after current languages like JavaScript and Python, developers can construct apps that operate on the EVM.

- **Solidity**

Solidity is an elevated object-oriented language for creating smart contracts. Smart contracts are programmes that control how accounts behave in the Ethereum state. Solidity is a programming language inspired by C++, Python, and JavaScript, and it was created with the Ethereum Virtual Machine in mind (EVM). Solidity is statically typed, and among its other capabilities, it enables inheritance, libraries, and sophisticated user specified types. Solidity allows you to design contracts for voting, crowdfunding, blind auctions, and multi-signature wallets, among other things. You should use the most recent version of Solidity when deploying contracts. This is due to the fact that breaking changes, as well as new features and bug fixes, are all introduced at the same time.

V. PROPOSED SYSTEM

Here, it is intended to propose a decentralized accreditation system i.e. digital certificate issuance, verification and validation using blockchain technology wherein ,the system issues the certificates to the students, storing the digitally signed transactions on the blockchain network. The certified document provided by the student to the employers/authorities contain a QR code and a unique number, that would be used to verify the certificate by the respective authorities. Unlike the current ,tedious manual process of verification this will be done very quickly. This DAPP would be a robust blockchain-based solution for quick and simple academic credential verification. The defined solution architecture seamlessly integrates with traditional credential system , as well as a threat model based on real-world fraud scenarios. We would develop a prototype that assures the authenticity of certificates and verifies it very quickly unlike the existing ,tradition process of verification. With this system the certificate bearer need not always carry the certificate along with, but only mention the QR code and unique identification number on the resume. This DAPP mitigates all the issues of the tradition accreditation system and its verification process as shown in figure 4.

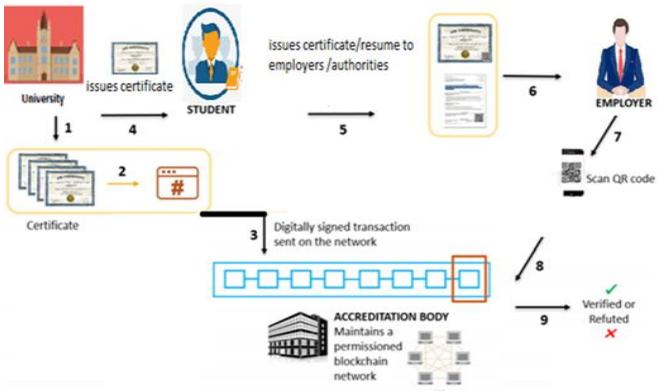

Fig.4

VI. RESULT AND DISCUSSION

The below given table discusses the result and performance analysis of blockchain platforms like Ethereum and Hyperledger Fabric which was essential before choosing the platform for implementation of the proposed system.[14]

Types	Ethereum	Hyperledger Fabric
Objective	To run the smart contracts	Develop blockchains for specific use cases
Use of Scripting Language	Solidity	Go
Currency used	Ether	Not applicable
Transaction size	Depends on the transactions, no max size	Configurable
Number of Instructions per second	limited	More than thousands of transactions per sec
Memory Utilization	Less memory	More memory resources are used
CPU utilization	Heavier	Not so heavier

VII. CONCLUSION

Credential fraud is a common and systemic practice that erodes confidence in educational institutions and jeopardizes student success, social growth, and it comes at a high price in terms of Regrettably, legacy credential authentication systems are inefficient, expensive, and time-consuming. Moreover, they are ineffective in combating such types of widespread corruption, such as educational institution and accreditation body fraud. Hence the proposed system is a comprehensive blockchain-based solution that combats widespread fraud while also providing significant usability and efficiency improvements over legacy systems. Also, the proposed system would have a number of advantages over other blockchain-based technologies that have been proposed in the literature and by industry.

Hence it is aimed to have a system that would be compatible with the current ecosystem to verify credentials, it also offers a mechanism for on-chain credential revocation, and not mandatory for the candidates or authorities to retain details like cryptographic credentials on file. The decentralized Accreditation System aims at, providing an effective anti-forge mechanism and also making the process of issuance, verification and validation of certificates digital using decentralized technology like Blockchain.

REFERENCES

1. INTERNATIONAL JOURNAL OF SCIENTIFIC & TECHNOLOGY RESEARCH VOLUME 9, ISSUE 03, MARCH 2020 ISSN 2277-8616 82 IJSTR©2020
2. Ei Mon Cho 1, Maharage Nisansala Sevwandi Perera22020 20th IEEE/ACM International Symposium on Cluster, Cloud and Internet Computing (CCGRID)
3. Efficient Certificate Management in Blockchain based Internet of Vehicles
4. Design and Implementation of Work Training Certificate Verification Based On Public Blockchain Platform 1st Irawan Afrianto Informatics Engineering Department, 2nd Yayan
5. Heryanto Informatics Engineering Department Efficient Distributed Admission and Revocation using Blockchain for Cooperative ITS Noureddine Lasla∗, Mohamed Younis§, Wassim Znaidi∗ and Dhafer Ben Arbia∗ ∗Qatar Mobility Innovations Center (QMIC), QSTP, Doha, Qatar
6. Cerberus: A Blockchain-Based Accreditation and Degree Verification System Aamna Tariq∗ , Hina Binte Haq , Syed Taha Ali‡ School of Electrical Engineering and Computer Sciences (SEECS), National University of Sciences and Technology (NUST), Islamabad, Pakistan.
7. Educational Certificate Verification System Using Blockchain Dinesh Kumar K, Senthil P, Manoj Kumar D.S INTERNATIONAL JOURNAL OF SCIENTIFIC & TECHNOLOGY RESEARCH VOLUME 9, ISSUE 03, MARCH 2020 ISSN 2277-8616
8. Marco Bali, 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.
9. 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).
10. 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.
11. S. Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System,2008; bitcoin.org/bitcoin.pdf. Hyperledger project,” [online] Available: https://www.hyperledger.org/ [Accessed on 5.07.2019]
12. IBM Blockchain based on Hyperledger Fabric from the Linux Foundation. Available from https://www.ibm.com/blockchain/hyperledger.html.
13. Nachiappan Michael Crosby, Pradan Pattanayak, Sanjeev Verma, Vignesh Kalyanaraman, "BlockChain Technology: Beyond Bitcoin", Applied Innovation Review, no. 2, Jun. 2016. [14] 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.
14. https://digitalscholarship.unlv.edu/cgi/viewcontent.cgi?article=4370&context=thesesdissertations

AUTHORS PROFILE

Dr. Dilip Motwani, I consider myself to be fortunate in taking a quantum leap into the field of Computer Engineering when it had begun to make an impact on the lives of people across the globe. I joined as a lecturer in an engineering college and started my work with complete hands on approach in designing and implementing computer network for all the laboratories in the college and it turned out to be a great learning experience. Completion of my post-graduation (ME) in Information Technology equipped me with a new skillset in Network Technologies and Mobile Computing through my project work entitled "Bandwidth Management”. While utilizing all my computer network skills I also learnt open source Linux operating system environment and mastered Cisco technology. Introduction to the ISP (Internet Service Provider) atmosphere further empowered my functionality in the computer networking area involving gateway configuration and installation of routers, LAN, Linux Server, etc. During the period, I got opportunity to work with organizations like CDAC and IGNOU as their program coordinator which also helped me in enhancing technical skills to great extent. My 21 year old association has made me acknowledge the reality of the Computer Engineering discipline where the only parameter that is constant is change.

Ms. Priti P. Bokariya, Today, Computer Engineering, discipline caters to the requirement of fields like Big Data Analytics, Computer Assisted Education, Bioinformatics, Cyber Security, Artificial Intelligence and Robotics After completion of my Engineering in 2010, I was placed in 2 multinational Companies. After acquiring some skillsets, I switched my profile into teaching and joined as a Lecturer in one of the Engineering colleges. Later I got placed in one of the known government aided diploma engineering college, viz. Shri Bhagubhai Mafatlal Polytechnic in Computer Department. Utilizing my interest in Programming I taught the subjects like C Programming, Object Oriented Programming in C++ and JAVA, Python Programming, Python for Hardware. However the subjects like Web Technology, E-commerce, RISC Processor ,Hardware Programming in Embedded C sharpened my skills and added to my experience. Also, I got admitted for masters in Computer Engineering in Vidyalankar Institute and ranked second in University with 9.67 CGPA. Gradually developed interest in Cryptocurrency like Bitcoin which led me research in the field of Blockchain. My special topic was “Scalability issues in Blockchain Technology” and hence developing a system as proposed in this paper using Blockchain Technology.

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication