Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14 Issue 05, May-2025

Engineering Degree Certification Verification using Blockchain Technology

Swayam Nayak
Dept. of ISE
BMSCE
Bengaluru, Karnataka

Swaroop T
Dept. of ISE
BMSCE
Bengaluru, Karnataka

Dr. M V Sudhamani Professor
Dept. of ISE
BMSCE
Bengaluru, Karnataka

Washif Ali
Dept. of ISE
BMSCE
Bengaluru, Karnataka

***Abstract*— This paper presents a novel implementation of a blockchain-based certificate management system that addresses the critical challenges of certificate forgery and verification in educational institutions. The proposed system leverages Ethereum smart contracts to create an immutable and transparent certificate registry, uniquely identified through University Seat Numbers (USN). The system implements a robust three-tier approval mechanism, requiring validation from the VTU (Visvesvaraya Technological University), Principal of BMSCE, and Department before certificate issuance. Through role-based access control and modern web technologies, the system provides a user-friendly interface for both institutions and recipients while ensuring instant verification capabilities. This implementation offers a practical and secure solution for educational institutions seeking to modernize their certificate management processes in the digital era. This work contributes to the growing field of blockchain-based educational credentialing by providing a practical, secure, and cost-effective solution for certificate management. It has been discussed in the paper along with results.**

***Keywords*— Digital Certificates, Blockchain, IPFS, Certificate Generation and Verification.**

I. INTRODUCTION

The blockchain is a distributed ledger i.e. is a system whereby replicated, shared, and synchronized digital data is geographically distributed across many sites, countries, or institutions with growing lists of records (or blocks) that are securely linked together via cryptographic hashes. Each block contains a cryptographic hash of the previous block, a timestamp, and transaction data. Since each block contains information about the previous block, they effectively form a chain (similar like a linked list data structure), with each additional block linking to the ones before it. Consequently, blockchain transactions are resistant to alteration because, once recorded, the data in any given block cannot be changed retroactively without altering all subsequent blocks and obtaining network consensus to accept these changes. The power of blockchain technology lies in its unique combination of features: security through cryptographic hashing, transparency through distributed ledger technology, decentralization through peer-to-peer networks, efficiency through automated consensus mechanisms, and traceability through immutable transaction records.

Despite these advantages of blockchain technology, educational certificate management systems face significant challenges in their current implementation. Traditional certificate systems are vulnerable to sophisticated forgery techniques, unauthorized alterations, and inefficient verification processes. The reliance on physical documents makes certificates susceptible to damage and loss, while manual verification creates problems in the credential validation pipeline. These vulnerabilities are particularly concerning in the educational sector, where the authenticity of academic credentials is crucial for both students and institutions.

Our proposed blockchain-based certificate management system addresses these vulnerabilities through a comprehensive security architecture. By implementing a unique University Seat Number (USN) identification system, we ensure that each certificate is uniquely identifiable and traceable. The system's three-tier approval mechanism, involving Principal, Department, and VTU validation, creates multiple checkpoints for certificate authenticity. This paper presents our system architecture, implementation details, and discusses how it contributes both to research and real-world applications.

II. INTRODUCTION

The paper focuses on building an immutable certificate generation as well as a validation system. For this, we have referred few previously published papers and works of the various individual in this field. Our Literature Survey mainly focused on Blockchain Technology, an advanced Storage System, and Digital Certificate Validations.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14 Issue 05, May-2025

In [1] provides in-depth knowledge regarding Blockchain. It introduces various terms regarding this technology and the important concept of a smart contract. In Blockchain, the hash of the data is stored in its preceding block, forming a chain of nodes. If data is altered, its hash will change, and it won't match the previous block's hash, indicating tampering.

In [2], "Blockchain and Smart Contract for Digital Certificate" presents a design involving three actors: institutions, students, and service providers. The drawback was the use of 'one hash as a key,' making it publicly accessible once the hash is known.

In [3], the paper "Tamper Proof Birth Certificate" proposes a system similar to the previous one but uses AES algorithm and IPFS for storage. Their focus was solely on birth certificates, but the drawback was that the original document was not stored, nor was there a mechanism for generating certificates online.

In [4], the paper titled "BlockIPFS (Blockchain-enabled Interplanetary File System for Forensic and Trusted Data Traceability)" explores the integration of IPFS with Blockchain. It compares traditional IPFS with Blockchain-enhanced IPFS, demonstrating that BlockIPFS performed better in upload, read, and download transactions.

In [5], the paper "Blockchain-Based Identity Verification Model" discusses a system where an Issuing Authority generates the document, a hashing algorithm processes it, and its value is stored. Unlike other systems with public hash keys, they improved security using asymmetric encryption.

In [6], "Enhancing Privacy in a Blockchain-based Public Key Infrastructure" addresses the privacy challenges in conventional PKI systems and presents a blockchain-based model using ECC and RSA. By making key updates unlinkable and using bloom filters for identity verification, the proposed system protects identity ownership without revealing key generation methods, enhancing both forward and backward privacy.

In [7], "Proposing a Blockchain-based Solution to Verify the Integrity of Hardcopy Documents", tackles document fraud by integrating cryptographic hashing, digital signatures, 2D barcodes, and OCR. By storing essential data on the blockchain and reducing barcode usage to one, the proposed solution improves document integrity verification without cluttering the document layout.

III. PROPOSED METHODOLOGY

A. Modules

1) Blockchain: Blockchain can better be understood as an immutable database and laid the foundation of the whole project. It provides a trusted environment where actions have done are visible and can't be tampered with.
2) Ethereum: The core foundation of the certificate system, implemented using Solidity 0.8.0, providing immutable and transparent certificate management. The smart contract handles certificate issuance, verification, and revocation through a secure, decentralized mechanism.
3) Certificate Registry Contract: A specialized smart contract implementing the OpenZeppelin's Ownable and ReentrancyGuard patterns, managing certificate lifecycle through unique USN (University Seat Number) identification and role-based access control.
4) Solidity: Solidity is an object-oriented programming language for writing smart contracts. It is used for implementing smart contracts on various Blockchain platforms, most notably, Ethereum. It is closely similar to Typescript but with more specific data types.
5) Web3.js: JavaScript library enabling frontend interaction with the Ethereum blockchain, facilitating real-time certificate operations and blockchain state management through MetaMask integration.
6) IPFS: Decentralized storage solution using Pinata's IPFS service for storing certificate metadata, ensuring data persistence and content-addressed storage of certificate information.
7) Firebase Authentication: Secure user authentication system implementing role-based access control, distinguishing between certificate issuers and recipients through email domain verification.
8) Ganache: Ganache is used for testing Solidity contracts on a personal Ethereum Blockchain. It by default provides an easy setup for spinning up a network with around ten users with each having 100 eths on their account. These accounts can be used to mimic the transactions between the users.
9) Truffle: Development framework managing smart contract compilation, testing, and deployment, with Ganache integration for local blockchain testing and development.
10) MetaMask: Browser extension integration enabling secure wallet connections and transaction signing, providing a secure interface for blockchain interactions.
11) Firebase Firestore: NoSQL database storing user profiles, certificate metadata, and system configuration, ensuring efficient data retrieval and management.
12) Gas Optimization Module: Smart contract implementation optimizing gas usage for certificate operations, with specific optimizations for certificate generation and verification.
13) Security Middleware: Express.js middleware implementing security best practices, including input validation, rate limiting, and secure session management for API endpoints.
14) Express.js: Node.js-based server implementation handling API endpoints for certificate generation, validation, and management, with middleware for authentication and request validation.

B. Project Description

The Blockchain Certificate System transforms educational credentialing by creating a secure and transparent way to manage academic certificates. Using a unique University Seat Number (USN) to identify each certificate, the system ensures that every academic achievement is uniquely recorded and protected against forgery. This innovative approach turns vulnerable paper documents into secure digital assets that cannot be tampered with.

The system's power comes from its integration of cutting-edge technologies. Smart contracts on the Ethereum blockchain provide an immutable certificate registry, while IPFS decentralized storage ensures permanent access to certificate data. A sophisticated role-based access control system distinguishes between authorized issuers and recipients,

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14 Issue 05, May-2025

ensuring that only legitimate educational institutions can issue certificates while maintaining student privacy.
Through Firebase authentication and MetaMask integration, the system provides a seamless experience for both institutions and students. Educational institutions can easily issue and manage certificates, while students can securely access and share their credentials. The system's architecture, built on OpenZeppelin's security patterns, ensures that every interaction is protected by industry-leading security measures. This implementation provides instant verification capabilities, allowing employers and educational institutions to verify certificate authenticity in seconds. By combining blockchain's immutability with modern web technologies, the system creates a practical solution that makes the process of managing and verifying academic credentials more secure, efficient, and trustworthy for everyone involved in the educational ecosystem.

1) System Design and Working
Our Blockchain Certificate System implements a secure, multi-level approval workflow for certificate management through Ethereum smart contracts and IPFS distributed storage. The system enforces a strict hierarchical approval process:
VTU (Visvesvaraya Technological University) serves as both the primary issuer and first-level approver, initiating the certificate generation process. Following VTU's approval, certificates proceed to the College Principal for second-level validation. The Department Head acts as the final approver, ensuring all academic and student-specific details are verified. Only after securing all three levels of approval can students access their certificates. The system implements a secure workflow where each certificate undergoes:

1. VTU initiation and first approval

2. Principal's institutional validation

3. Department's final verification

4. Blockchain storage with IPFS metadata

5. Student access and verification capabilities

This architecture ensures:

- Immutable certificate records
- Complete approval audit trail
- Tamper-proof verification process
- Efficient multi-stakeholder workflow
- Secure certificate management.

IV. IMPLEMENTATION DETAILS

The implementation of the blockchain-based certificate management system, as shown in Figure 1, elaborates on a smart contract deployed on the Ethereum blockchain. This contract manages the entire certificate lifecycle, uniquely identifying each certificate with a University Seat Number (USN) and enforcing a three-tier approval process involving the VTU, Principal, and Department nodes. Only after all approvals is the certificate made available to the student.

Certificate data and hashes are securely stored on IPFS, ensuring tamper-proof and persistent access, while the USN Registry prevents duplication. The backend, built with Express.js, handles API requests and integrates security middleware for safe operations. User authentication and role management are provided by Firebase Authentication, ensuring only authorized users can issue or access certificates. The frontend leverages Web3.js and MetaMask for secure blockchain interactions, allowing users to manage and verify certificates easily. Development and testing are streamlined using Truffle and Ganache, while Firebase Firestore manages user and certificate metadata. This integrated approach ensures a secure, efficient, and transparent certificate management process.

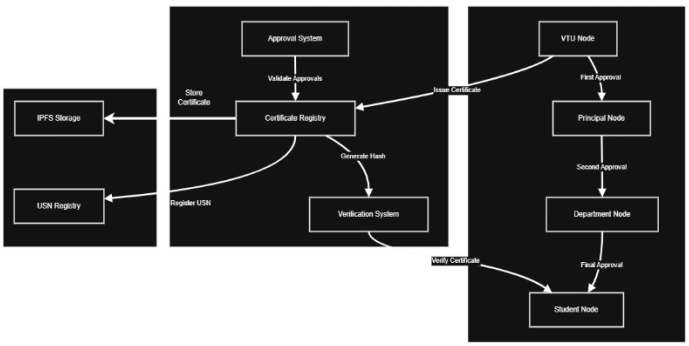

Figure 1. System Architecture

RESULTS AND DISCUSSIONS

Following are some of our implementation results:
1) Dashboard (General/Student):
Figure 2 captures the result screen after VTU initiates the issuance of a certificate. It confirms the successful creation of a new certificate record and provides details such as the student's information, certificate ID, and transaction hash. This confirmation step is essential for transparency, as it allows VTU to verify that the certificate has been correctly registered on the blockchain and is ready for the next stage of approval.

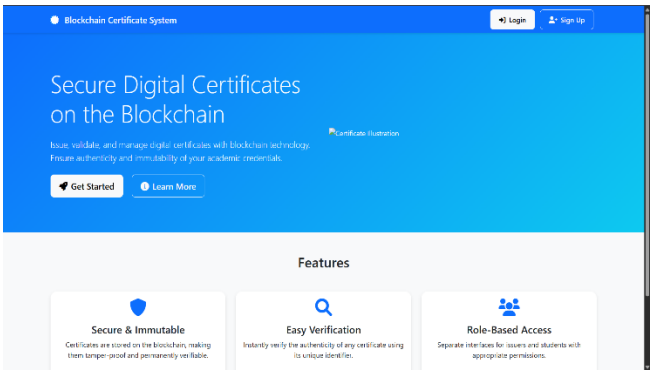

Figure 2. Dashboard for logged out users

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14 Issue 05, May-2025

2) Login Page:

Figure 3 captures the result screen after VTU initiates the issuance of a certificate. It confirms the successful creation of a new certificate record and provides details such as the student's information, certificate ID, and transaction hash. This confirmation step is essential for transparency, as it allows VTU to verify that the certificate has been correctly registered on the blockchain and is ready for the next stage of approval.

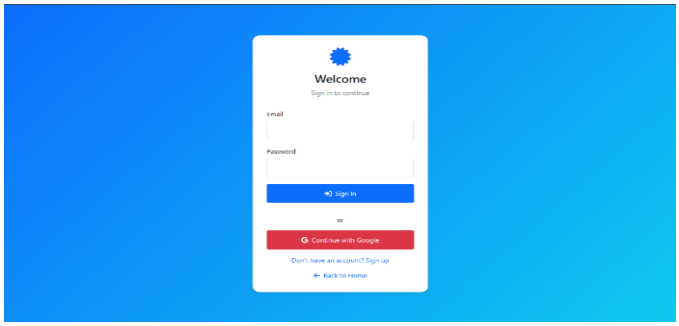

Figure 3. Login Page

3) VTU Dashboard:

Figure 4 captures the result screen after VTU initiates the issuance of a certificate. It confirms the successful creation of a new certificate record and provides details such as the student's information, certificate ID, and transaction hash. This confirmation step is essential for transparency, as it allows VTU to verify that the certificate has been correctly registered on the blockchain and is ready for the next stage of approval.

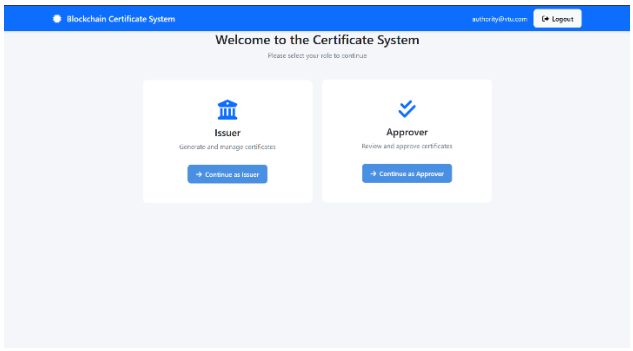

Figure 4. Dashboard for VTU (logged in as VTU)

4) VTU Issue Certificate Result:

Figure 5 captures the result screen after VTU initiates the issuance of a certificate. It confirms the successful creation of a new certificate record and provides details such as the student's information, certificate ID, and transaction hash. This confirmation step is essential for transparency, as it allows VTU to verify that the certificate has been correctly registered on the blockchain and is ready for the next stage of approval.

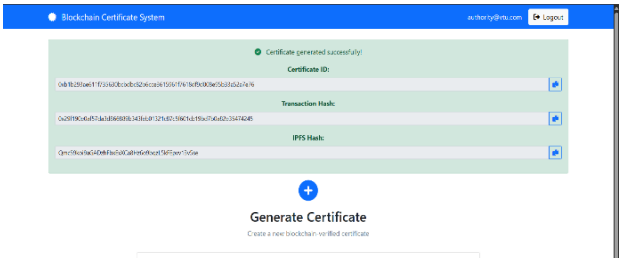

Figure 5. Successful Issuance of Certificate by VTU

5) VTU Certificate Approval Screen :

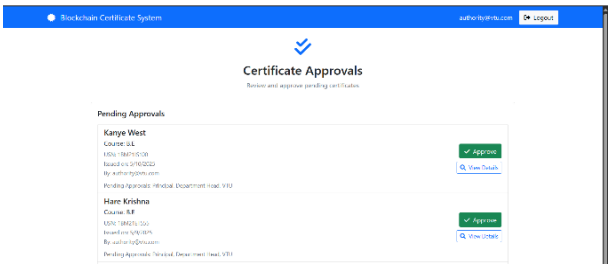

Figure 6. Certificate Approval Screen for VTU

6) Principal Approver List:

Once a certificate is issued by VTU, it appears in the principal's approver list. Figure 7 shows the following. This interface displays all certificates awaiting the principal's review and approval, along with relevant details for each entry. The principal can examine the certificate data, verify its accuracy, and either approve or reject the request. This step enforces institutional oversight and ensures that only validated certificates progress further in the workflow.

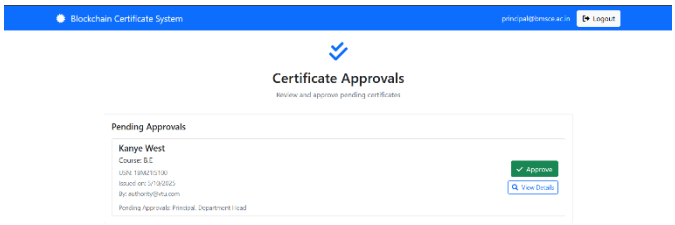

Figure 7. Successful Approval by the Principal of the college.

7) Department Approver List-

Figure 8 the principal's approval, certificates move to the department head's approver list. This dashboard provides department heads with a clear view of all certificates pending their final validation. The department head reviews academic details and confirms the authenticity of each record before granting approval. This additional layer of scrutiny strengthens the system's reliability and prevents unauthorized or erroneous certificate issuance.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14 Issue 05, May-2025

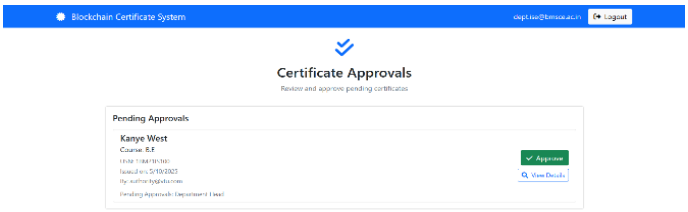

Figure 8. Information Science Department Certificate list

8) Certificate After All Approvals (Student View):

After receiving approvals from VTU, the principal, and the department head, the certificate becomes accessible to the student. The student's dashboard displays the finalized certificate, complete with a unique identifier and verification link. Students can view, download, and share their certificates, confident in the knowledge that their credentials are securely stored and verifiable on the blockchain. Figure 9 and 10 shows the following.

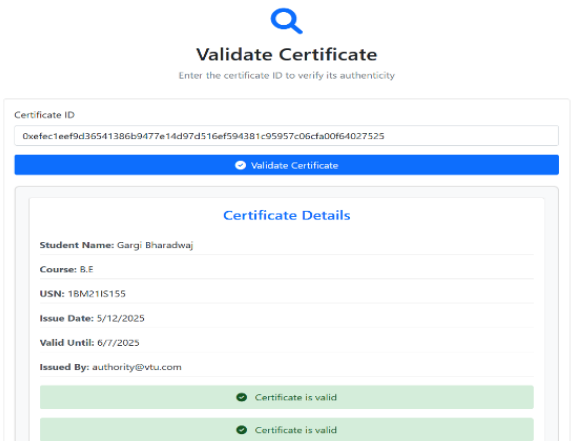

Figure 9. Certificate viewed by the student after issuance and all approvals

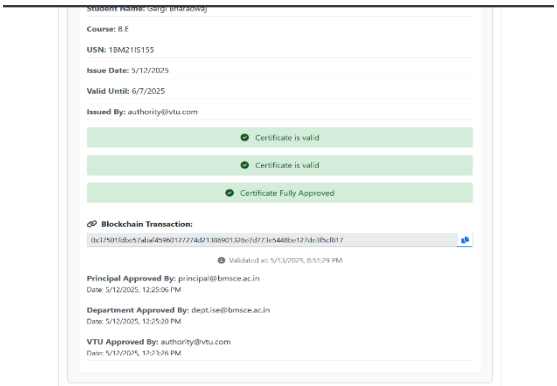

Figure 10. Certificate viewed by the student showing the approved nodes and timestamps

9) Ganache Desktop – Contract Creation –

Figure 11 displays the Ganache Desktop environment, which is used to simulate the Ethereum blockchain during development and testing. The interface provides a comprehensive view of all blockchain transactions related to the certificate system, including the initial deployment of the CertificateRegistry.sol smart contract and subsequent contract calls for certificate issuance, approval, and verification. Each transaction is transparently logged, showing details such as sender, receiver, gas usage, and transaction status. This real-time record of contract creation and operational calls serves as an immutable audit trail, demonstrating the system's transparency, security, and the integrity of all certificate-related activities on the blockchain

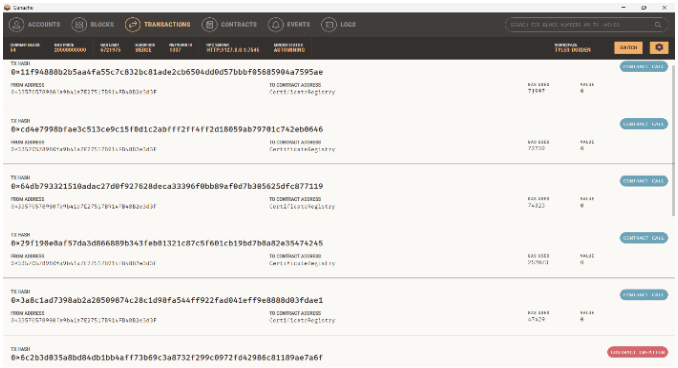

Figure 11. Contract creation/calls of the process.

CONCLUSION AND ENHANCEMENTS

The blockchain-based certificate management system presented in this work offers a secure, transparent, and efficient solution to the longstanding challenges of academic credential verification. By leveraging Ethereum smart contracts, decentralized IPFS storage, and a robust multi-tier approval process, the system ensures that every certificate is uniquely identifiable, tamper-proof, and instantly verifiable. The integration of modern authentication and user management tools further enhances security and usability, making the system practical for real-world adoption by educational institutions. Overall, this approach not only eliminates the risk of forgery and manual errors but also empowers students and institutions with a reliable and future-ready credentialing platform.

Looking ahead, several enhancements can further strengthen and expand the system's capabilities. Integrating support for multiple blockchains could improve scalability and reduce operational costs. The addition of advanced analytics and reporting tools would help institutions track certificate issuance and verification trends. Incorporating biometric or digital identity verification could further secure user authentication. Finally, developing a mobile application and expanding interoperability with other educational and governmental platforms would make the system even more accessible and versatile, paving the way for widespread adoption and a truly global standard in academic credential management.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14 Issue 05, May-2025

REFERENCES

[1] Zibin Zheng , Shaoan Xie, Hong-Ning Dai, Xiangping Chen , ” An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends”, IEEE 6th International Congress on Big Data, 2017.

[2] Jiin-Chiou, Narn-Yih Lee, Chien Chi, YI-Hua Chen, “Blockchain and Smart Contract for Digital Certificate,” Proceedings of IEEE International Conference on Applied System Innovation 2018.

[3] Maharshi Shah, Priyanka Kumar, “Tamper Proof Birth Certificate Using Blockchain Technology”, International Journal of Recent Technology and Engineering (IJRTE), Volume-7, Issue-5S3, February 2019.

[4] Emmanuel Nyaletey, Reza M. Parizi, Qi Zhang, Kim-Kwang Raymond Choo, “BlockIPFS - Blockchain-enabled Interplanetary File System for Forensic and Trusted Data Traceability”, IEEE International Conference on Blockchain, 2019.

[5] Gunit Malik, Kshitij Parasrampuria, Sai Prasanth Reddy, Dr. Seema Shah, “Blockchain Based Identity Verification Model”, International Conference on Vision Towards Emerging Trends in Communication and Networking (ViTECoN), 2019.

[6] Amalan Joseph Antony A, Kunwar Singh, “Enhancing Privacy in a Blockchain-based Public Key Infrastructure”, Third ISEA Conference on Security and Privacy (ISEA-ISAP), IEEE, 2020.

[7] Sthembile Mthethwa, Nelisiwe Dlamini, Dr. Graham Barbour, “Proposing a Blockchain-based Solution to Verify the Integrity of Hardcopy Documents”, Council for Scientific and Industrial Research (CSIR), IEEE, 2018.Malik, Kshitij Parasrampuria, Sai Prasanth Reddy, Dr. Seema Shash, “ Blockchain Based Identity Verification Model”, Internation Conference on Vision Towards Emerging Trends in Communication and Networking(ViTECoN), 2019