IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Blockchain Technology For Secure Digital Certificate Generation And Verification

[1]Kunal Godase, [2]Omkar Ghate, [3]Swapnil Kale, [4]Saurabh Ghadage, [5]Prof. Sudhakar Jadhav

[1,2,3,4]Students, I.T. Department, N.Y.S.S. Datta Meghe College Of Engineering, Airoli

[5]Professor, I.T. Department, N.Y.S.S. Datta Meghe College Of Engineering, Airoli

Abstract: As the number of graduates increases each year, guaranteeing the integrity and security of academic certificates has emerged as a significant challenge. Conventional certificate validation techniques are susceptible to forgery, loss, and inefficient, posing a challenge to institutions and employers to verify credentials accurately. To mitigate this problem, we present a blockchain-aided certificate issuance and verification system that exploits the decentralized and immutable characteristics of the blockchain technology. Only verified educational institutes, which are authorized by an admin, can create and give certificates in this system, which maintains authenticity and restricts unwarranted access. The certificates are securely stored by generating its hash value, and its IPFS (InterPlanetary File System) value and these values are stored on the blockchain. This allows certificates to be verified instantly without a central authority. In contrast to conventional approaches, the system guarantees data integrity, immutability, transparency, and minimizes the potential of certificate forgery. The proposed approach improves the trustworthiness of academic credentials and offers a automated, and tamperproof mechanism for instant certificate verification.

Index Terms **- Blockchain, Digital certificate, Generation, Validation.**

I. INTRODUCTION

Academic certificates play a crucial role in verifying a student's qualifications for higher education and employment. However, the increasing incidents of certificate forgery and the inefficiencies of manual verification pose significant challenges. Institutions and employers struggle to authenticate credentials accurately, leading to cases where unqualified individuals exploit loopholes in the system. Traditional paper-based certificates are also prone to loss and damage, further complicating the verification process. Blockchain technology provides a decentralized and tamper proof solution for these concerns. This paper proposes a blockchain based certificate generation and validation system in which only authorized educational institutes which are approved by an admin can create certificates. This involves storing the hash value and IPFS (InterPlanetary File System) link of each certificate directly onto the blockchain; ensuring that no one can fake or change the certificate. Since blockchain is immutable, a certificate once recorded cannot be changed and can be verified quickly, securely and worldwide. The incorporation of blockchain not only strengthens these initiatives, but also adds greater transparency, security, and trust to the process of issuing academic certificates. Smart contracts are used for automated and verifiable transactions, minimizing reliance on centralized third parties. This study strives to deliver a secure and trusted alternative approach to academic certificate management that overcomes the deficiencies of traditional methods, while also offering the possibility of access to stored data, as well as proof of security.

II. LITERATURE REVIEW

The first research paper, Online certificate validation using blockchain [1], describes the reliability and transparency of using Ethereum blockchain for document validation. The paper cites disadvantages to traditional centralised storage of certificates, which makes them vulnerable to hacking and duplication. The

system uses blockchain technology to eliminate scalability and trust issues with the help of powdered data storage and SHA-256 hashing.

The second research paper, Generating E-Certificate and Validation using Blockchain [2], explains about secure generation and validation of e-certificates. It highlights an aspect of the current systems: lack of transparency and verifiability, which is what makes it possible to forge documents. Built on the blockchain with smart contracts, the proposed solution solves secure updates and anti counterfeiting. Hash values authenticates the certificates store.

The third research publication, A Blockchain-based Authentication and Verification System for Academic Certificate using QR Code and Decentralized Applications [3], proposes a decentralized application (DApp) which uses Ethereum blockchain, IPFS, and smart contracts. By introducing QR codes for efficient verification, this system improves the security and effectiveness of certificate authentication. The paper also addresses issues around smart contract vulnerabilities, data privacy, and private key management. Suggested mitigations include smart contract audits and IPFS for secure storage.

The fourth research paper, Blockchain-Based Certificate Validation System [4], describes a model for verifying the tamper-proof feature of digital certificates with the use of blockchain. While the paper itself does not make direct references to issues of fake certificates, tampering of documents, or secure backend smart contracts, it addresses these issues indirectly. The system is secured by verifying any certificate against the blockchain and safely storing the certificates. The study relies on Proof-of-Work consensus mechanism and The SHA-256 hash function to guarantee data integrity and confidentiality.

Together, these research studies highlight the benefits of utilizing blockchain technology to improve the security, authenticity, and transparency of certificate validation systems. Together they provide insight into different methods of implementation, obstacles to integration, and potential solutions for decentralized digital certificates in education.

III. Proposed Methodology

1. System Workflow

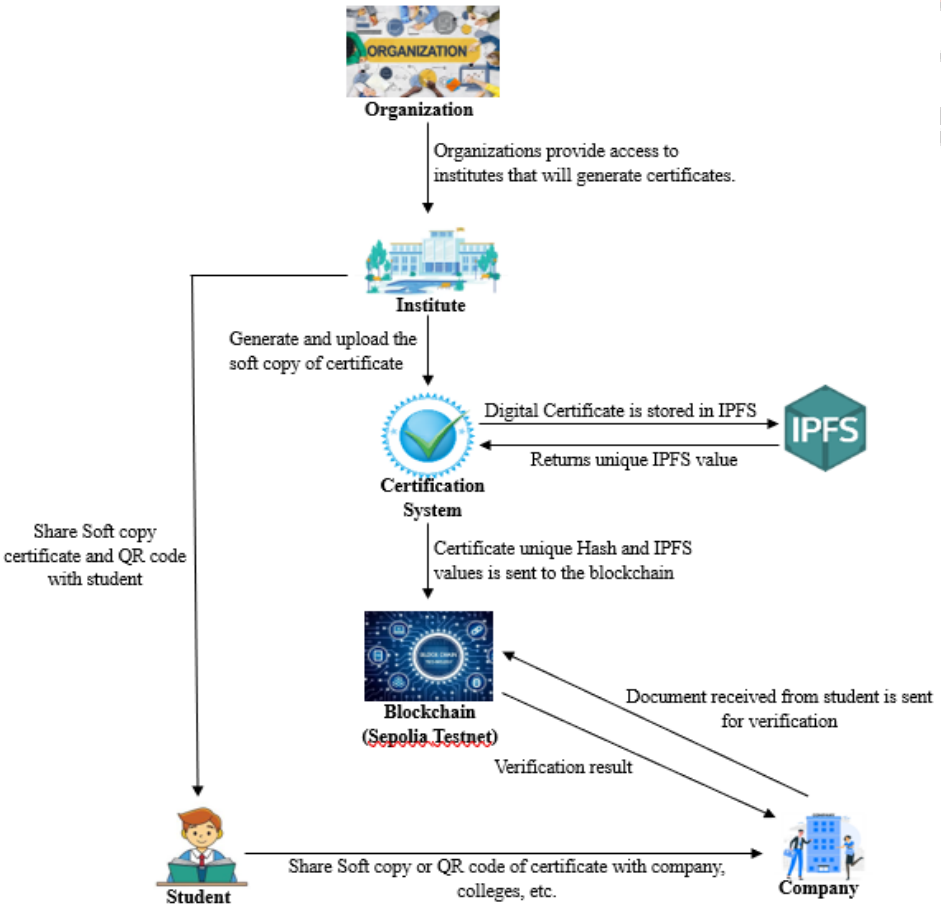

Figure 1: Workflow of the system

With the help of Blockchain (Sepolia Testnet) and IPFS, the presented method achieves a safe certificate generation and validation mechanism in a decentralized way. Authorized access is given to institutes by organizations admin, who creates digital certificates for students. A certificate can be created by the Certification System, and it is saved in IPFS, obtaining an unique hash on the IPFS. This hash, along with the cryptographic hash of the certificate are stored on Sepolia Testnet for immutability and to prevent tampering. Students are also provided a soft copy certificate along with a QR code which is shared separately. If verification is required, the verifier scans the QR code and is then redirected to a verification page from which the hashed document is retrieved from the blockchain and matched with the certificate provided. If their hashes match, then the certificate is valid. With Sepolia Testnet providing decentralized security, IPFS for distributed storage, cryptographic hashing for integrity, and QR code-based verification, this approach creates a tamper-proof, transparent, and efficient certificate management system.

2. Tools and Technologies used

1) Blockchain

Blockchain is a decentralized digital ledger that securely stores records across a network of computers in a way that is transparent, immutable, and resistant to tampering [5]. This novel technology makes use of cryptographically interconnected data blocks. Immutability is a distinguishing feature of decentralized blockchains, which ensures that once information is recorded, it cannot be altered.

2) Sepolia Testnet

Sepolia is a testing network for Ethereum that started in 2021 and operates separately from the main network (mainnet) while closely mimicking its conditions. Sepolia is an Ethereum testnet that provides a stable environment for developers to test and deploy their applications before launching on the Ethereum mainnet [6].

3) Smart Contract

Smart contracts are digital contracts stored on a blockchain that are automatically executed when predetermined terms and conditions are met [7]. Smart Contract is a self-operating program executing the procedures included in a blockchain transaction. Once executed, the transactions cannot be manipulated and are traceable. Developers can create smart contracts in a variety of programming languages, including C++, Java, and Solidity (similar to Typescript).

4) Solidity

Solidity is a brand-new programming language created by Ethereum which is the second-largest market of cryptocurrency by capitalization, released in the year 2015 and led by Christian Reitwiessner [8].

5) IPFS (Interplanetary File System)

IPFS is a modular suite of protocols for organizing and transferring data, designed from the ground up with the principles of content addressing and peer-to-peer networking [9]. To minimize storage costs on the blockchain, only the certificate hash and IPFS link are recorded instead of the full certificate. With the unique hash, the system downloads the certificate from IPFS, enabling the verification from anywhere.

6) SHA3 Algorithm

The SHA or SHA-3 (Secure Hash Algorithm 3) is known to be the latest member of the SHA family of the secure hash algorithm stands it is published by the NIST on the year 2015 [10].

7) Metamask

MetaMask is a popular and established browser extension which functions as a cryptocurrency wallet that connects to the Ethereum blockchain [11]. t allows for users to be authenticated so that only authorized entities (like institutions) can write the certificates. It provides signing of blockchain transactions securely and can make certificate issuance and verification a seamless experience. Users can securely sign blockchain transactions, which also makes issuing and verifying certificates smooth.

8) ReactJS

ReactJS is a component-based JavaScript library used to build dynamic and interactive user interfaces [12]. It allows the user to easily generate, upload, and verify certificates on a responsive and dynamic frontend. All the verification results can be displayed in real time by fetching data from the blockchain using react. Designed for use with the Metamask wallet, users of the system can connect their wallets and engage effortlessly.

9) NodeJS

NodeJS is used to build the backend of the system that takes care of API requests, blockchain interaction, and file uploads. It facilitates the React frontend and Ethereum blockchain interaction while processing the smart contract transactions. It also interacts with IPFS, uploading and retrieving certificates. The backend facilitates secure communication with the blockchain on the user's behalf, improving the overall reliability of the system.

10) VS Code

The smart contracts, backend code, and frontend components are written and debugged with Visual Studio Code (VS code), which is the main IDE (integrated development environment) used. It extends support to Solidity, JavaScript, and NodeJS for a seamless development experience. VS Code allows developers to handle smart contract deployment, interact with the blockchain, and test the entire system efficiently.

3. System Description

1) Admin Module

The admin has the highest level of control over the system. The Admin Module is responsible for managing institutions by granting or revoking their access based on eligibility. The admin ensures that only verified institutes are allowed to issue certificates, maintaining the integrity of the system. However, the admin does not have access to the certificate generation page and cannot generate certificates. Their role is strictly limited to overseeing institute permissions, ensuring that only authorized entities can issue certificates.

2) Institute Module

The Institute Module allows registered institutes to generate certificates for students, ensuring authenticity and security through blockchain integration. Institutes have the capability to generate certificates for multiple students at a time, streamlining the issuance process. Additionally, they can delete issued certificates if necessary, ensuring better control and management of records. Once generated, the certificate details are stored on the blockchain, and the document itself is uploaded to IPFS for decentralized storage, maintaining integrity and preventing tampering.

3) Verifying Authority

The Verifying Authority Module is designed for anyone who needs to validate a certificate's authenticity. This can include students, employers, educational institutions, or any organization that requires certificate verification. Users can upload the certificate to the system, which will check it against blockchain records to determine whether it is legitimate or fraudulent. No special access or authentication is required, allowing seamless verification for anyone with a certificate. This ensures transparency, prevents the use of fake certificates, and simplifies the verification process for various stakeholders.

4) Certificate Generation and Deletion

The Certificate Generation Module allows institutes to create certificates efficiently using either predefined templates or custom templates of their choice. Institutes can generate multiple certificates at once by uploading an Excel file containing student details, streamlining the certificate issuance process. Once generated, the certificates are securely stored on IPFS, ensuring decentralization and immutability. The institutes then shares the certificate details with the respective students, providing them with a secure and verifiable digital certificate. The Certificate Delete Module allows institutes to remove issued certificates from the system when necessary. If a certificate is mistakenly generated or needs to be revoked due to errors, the institute has the authority to delete it. However, since blockchain records are immutable, the certificate's transaction history remains on the blockchain, ensuring transparency and traceability. This module helps maintain an accurate and updated list of valid certificates, preventing any misuse of outdated or incorrect credentials.

5) Certificate Upload

The Certificate Upload Module ensures secure storage and integrity verification of issued certificates. When a certificate is uploaded, its hash is generated using the SHA 3 algorithm, and the hashed value is stored on the blockchain to prevent tampering. Furthermore, the certificate is stored on IPFS (InterPlanetary File System), with its corresponding IPFS hash recorded on the blockchain. This approach guarantees that the certificate remains immutable, decentralized, and easily verifiable.

6) Certificate Verification

The Certificate Verification Module enables verifiers, including students, employers, and organizations, to authenticate certificates. To verify, the user uploads the certificate, and its hash value is computed using the SHA-3 algorithm. This generated hash is then compared with the stored certificate hashes on the blockchain. If a match is found, the system retrieves the certificate details and confirms its authenticity. If no match is found, the system returns an output stating that the certificate could not be verified, indicating that it may be fraudulent or not registered in the system. This ensures a secure and tamper proof verification process without requiring any special access.

IV. IMPLEMENTATION

Figure 2 shows the system's Home Page. It provides an introduction to the platform, emphasizing secure document verification using blockchain technology. The page includes a "Connect Wallet" button, allowing users to link their MetaMask wallet for blockchain interactions. Additionally, there is a "Go Verify" button to navigate to the verification page.

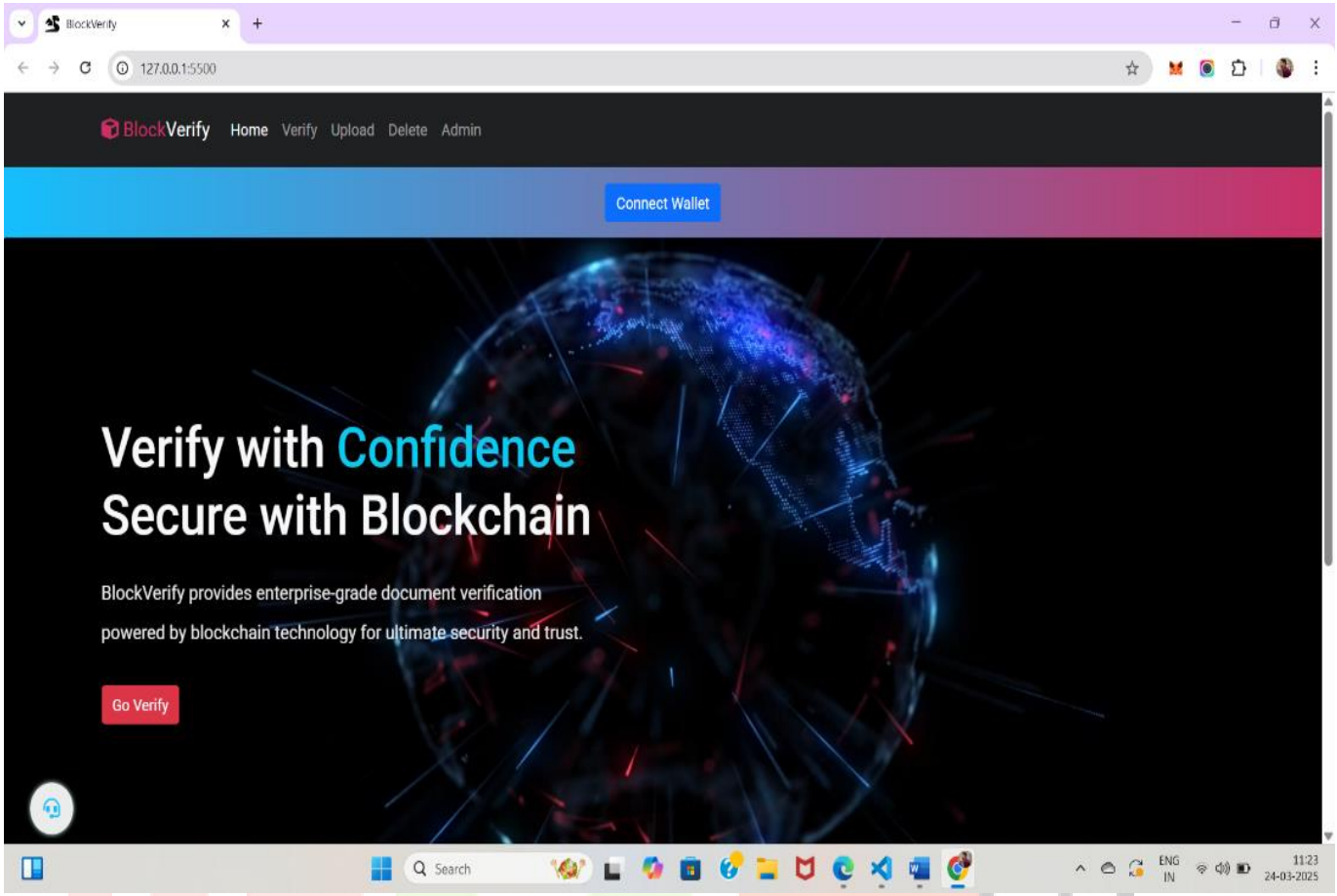

Figure 2: Home page of the system

Figure 3 shows the system's Admin Page. The admin can add, delete, or edit institution details using the provided interface. The admin can use the "Add Exporter" button to grant certificate issuance rights to an institution, the "Delete Exporter" button to revoke access, and the "Edit Exporter" button to update institution details.

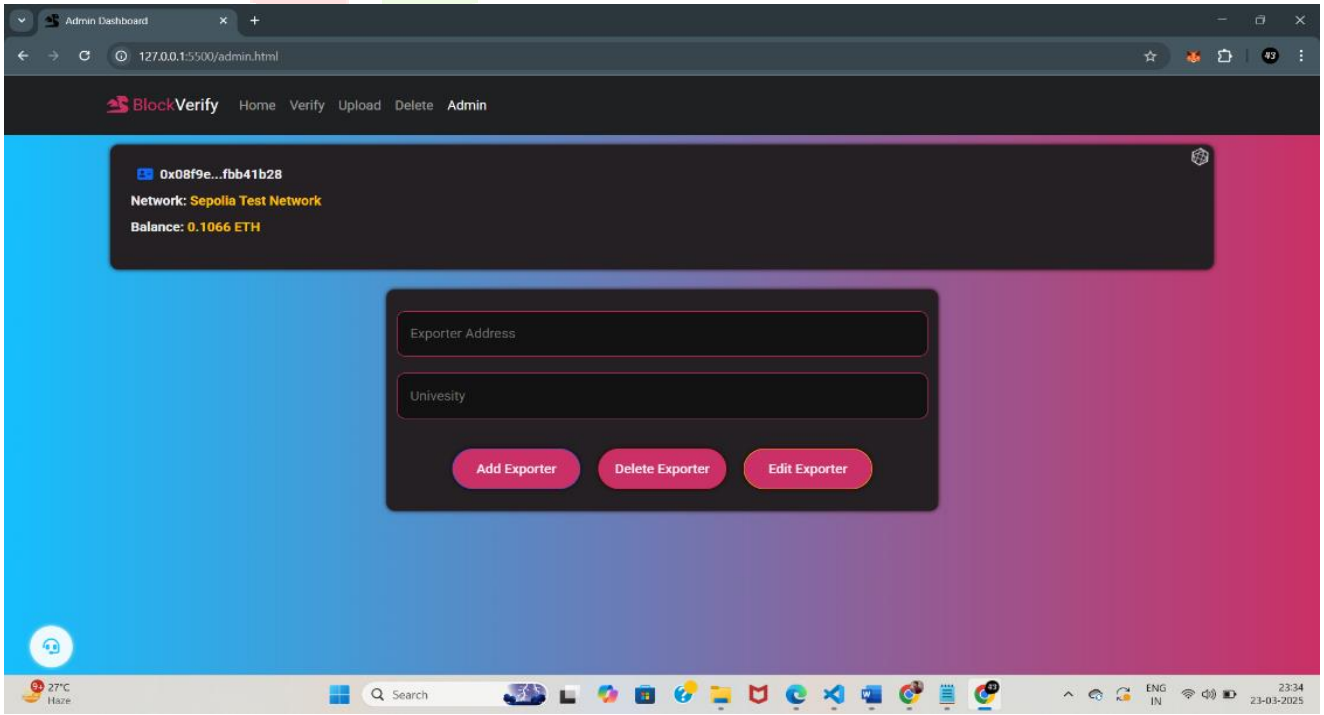

Figure 3: Admin page

Figure 4 shows the system's Certificate Generation page which enables institutions to create and customize certificates efficiently. Users can select predefined templates or design their own, adjusting font styles, sizes, and formatting options. The system supports bulk certificate generation by allowing the upload of CSV/Excel files containing multiple student details. Once generated, the certificates can be downloaded as PNG or pdf files.

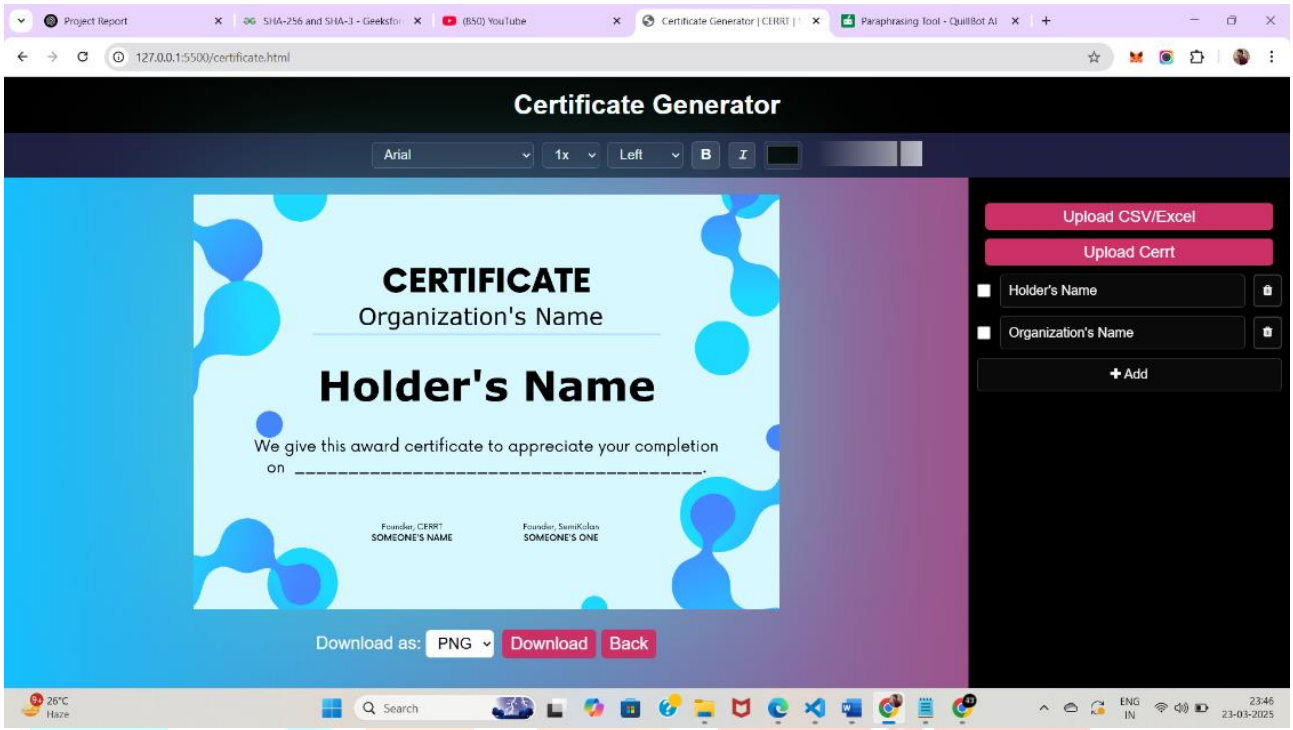

Figure 4: Certificate Generation Page

Figure 5 shows the system's certificate upload page. The Upload Document page in the blockchain-based certificate system allows authorized institutes to securely upload and store documents on the blockchain.

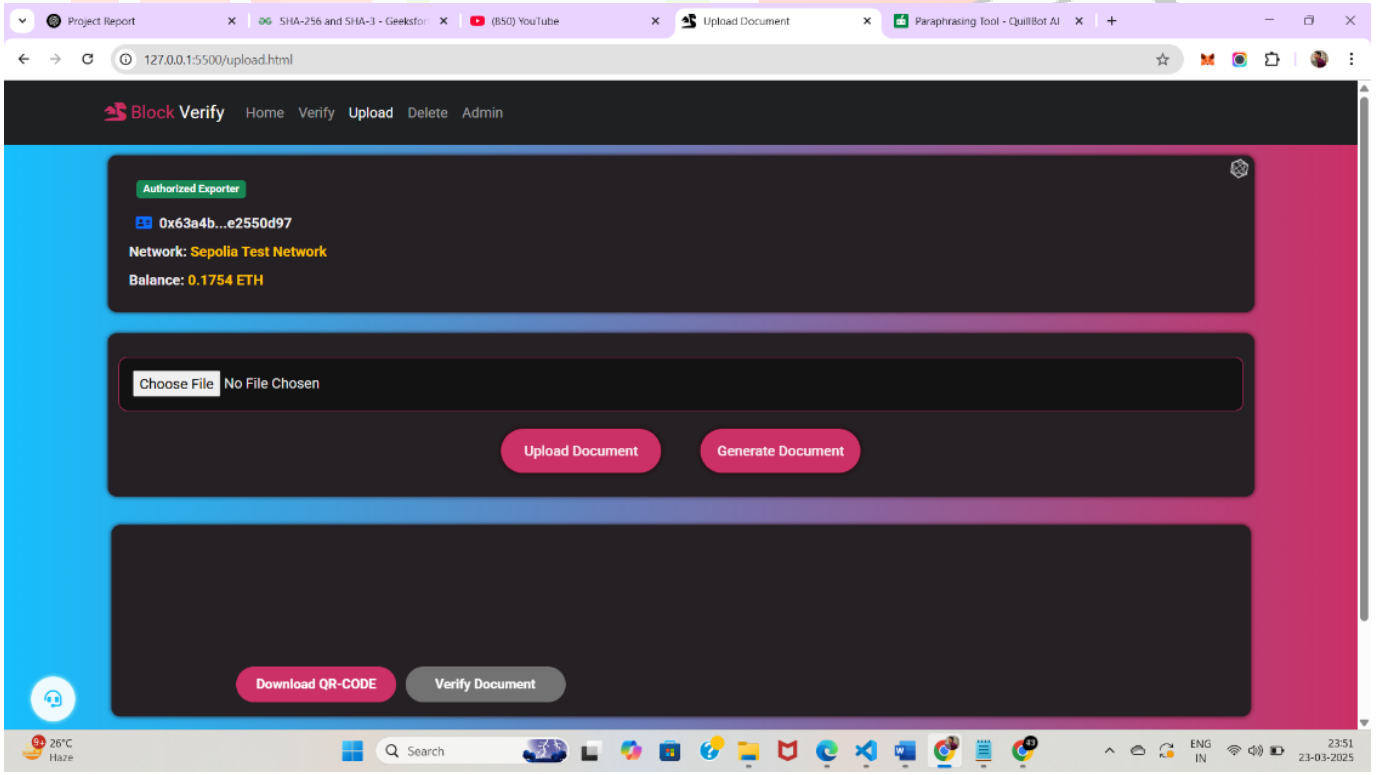

Figure 5: Certificate Upload Page

Figure 6 shows the system's certificate delete page. The Delete Document page in the blockchain-based certificate system enables authorized users to remove document records from the blockchain.

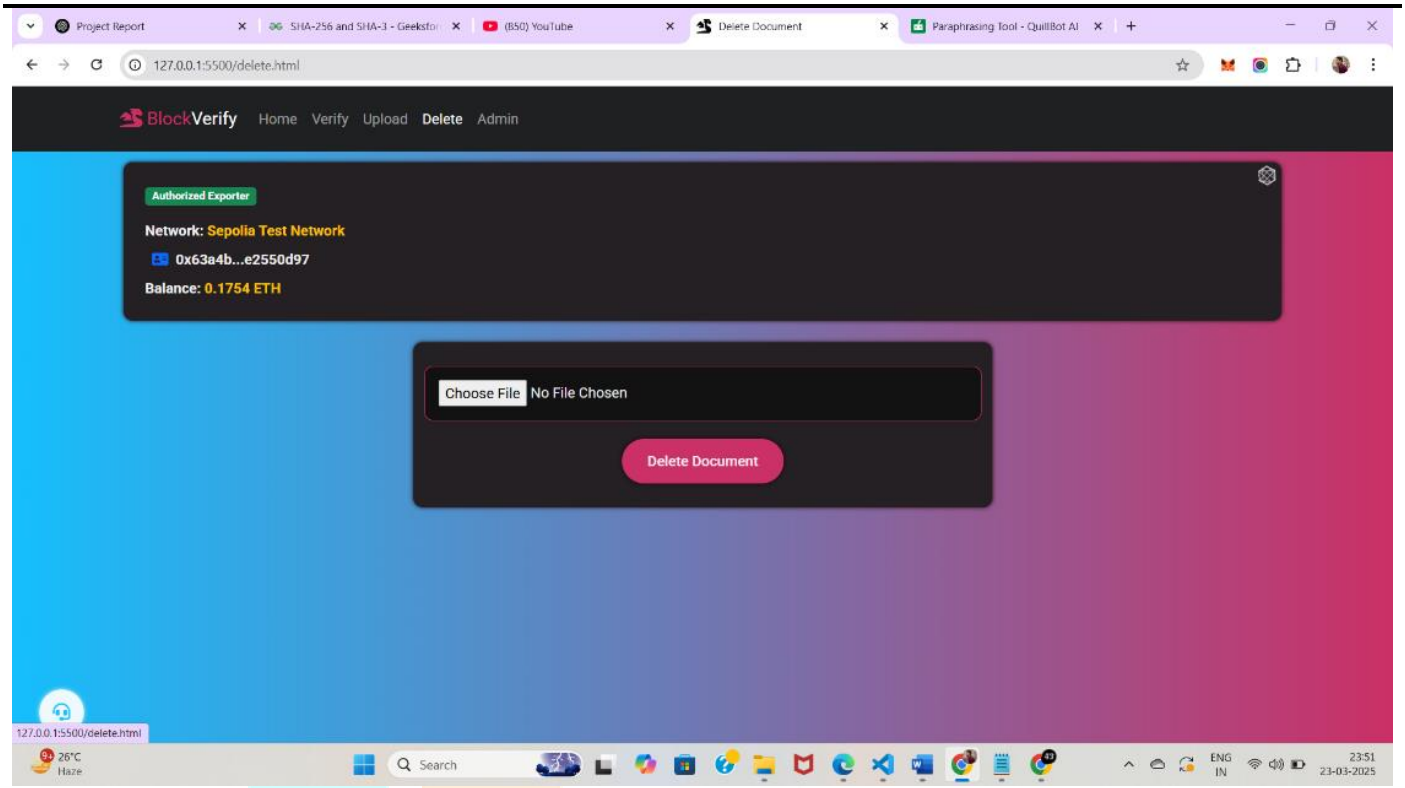

Figure 6: Certificate Delete Page

Figure 7 shows the system's verification page. The Verify Document page in your blockchain-based certificate system allows users to confirm the authenticity of a document.

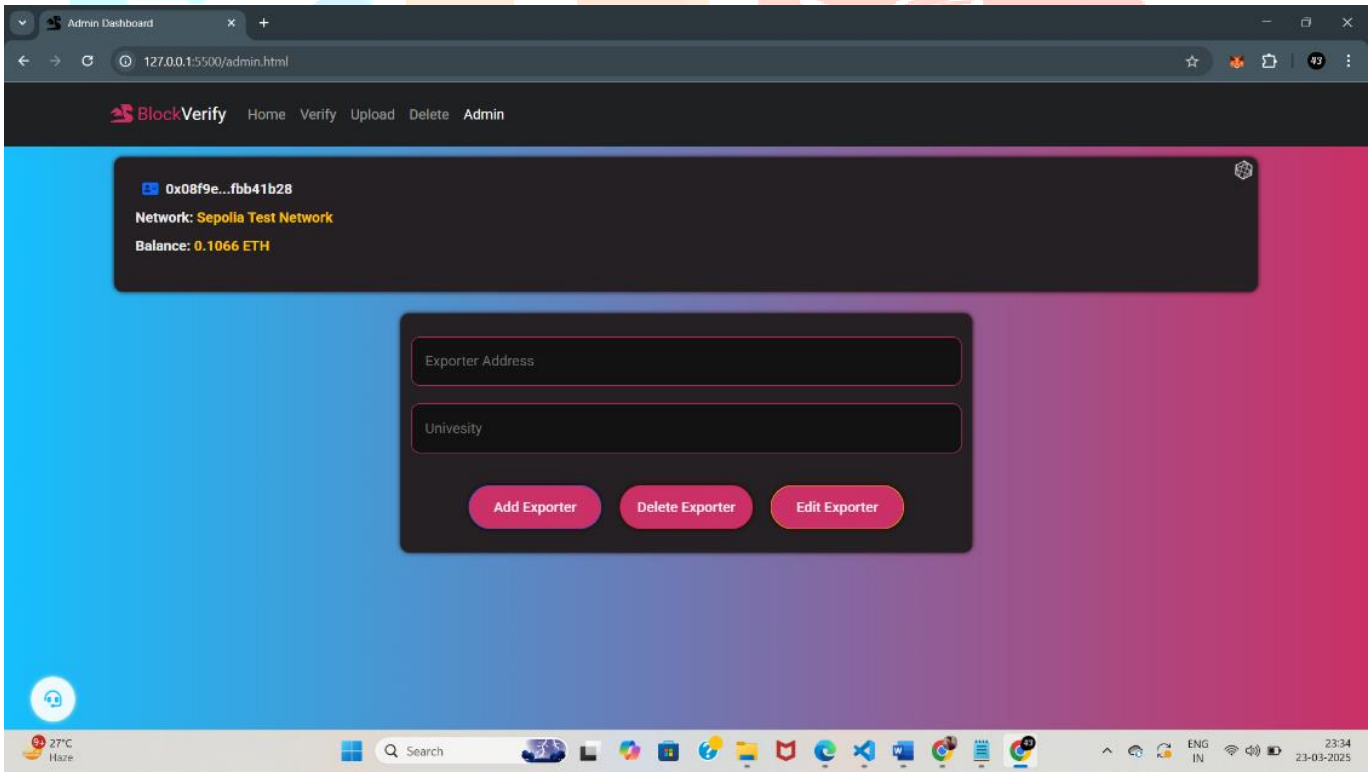

Figure 7: Verification Page

Figure 8 shows your Etherscan transaction history for the Sepolia Testnet.

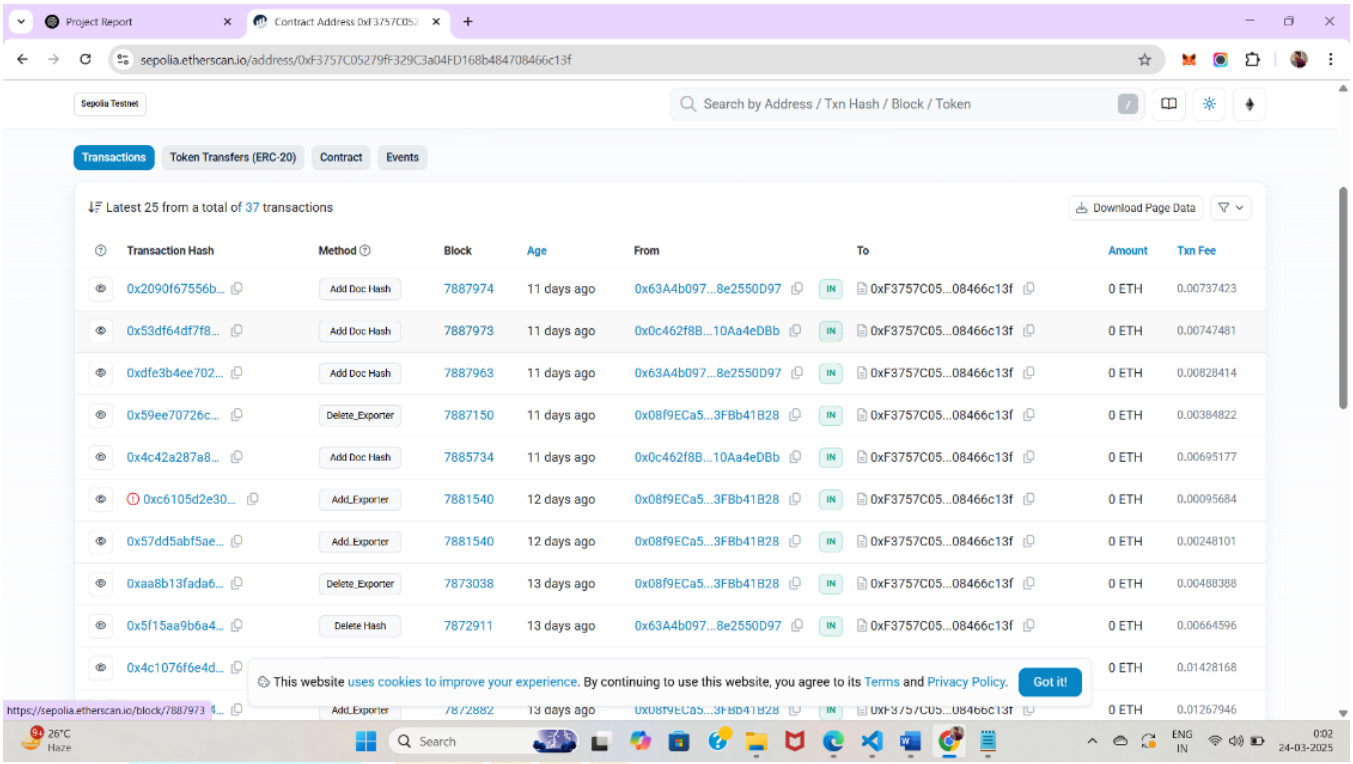

Figure 8: Sepolia Testnet page

V. CONCLUSION

In this project, we successfully designed and implemented a blockchain-based certificate generation and validation system, ensuring secure and tamper-proof document authentication. Certificate hashes are stored immutably on theSepolia Testnet through smart contracts, IPFS is used for decentralized storage, and Metamask is used for user authentication. Frontend (React + Node.Js) that enables users to seamlessly upload, verify, and delete certificates, and promotes transparency and security. With this, we have showcased the capabilities of blockchain in document verification and provided an alternative way to fight against frauds. This initiative lays the groundwork for a transparent and decentralized digital certification framework, paving the way for blockchain's broader integration in document management sectors.

VI. REFERNCES

VII.

[1] Shanmuga Priya R and Swetha N, "Online Certificate Validation Using Blockchain," *International Journal Of Advanced Networking & Applications.*

[2] Rohan Hargude, Ghule Ashutosh, Abhijit Nawale and Pro.Sharad Adsure, "Generating E-Certificate and Validation using Blockchain," *International Journal of Creative Research Thoughts (IJCRT)*, vol. 09, no. 07, 2021.

[3] Shivam Gangwar and Anushka chaurasia, “Blockchain-based Authentication and Verification System for Academic Certificate using QR Code and Decentralized Applications,” *International Journal of Computer Applications*, 2024.

[4] R. Suganthalakshmi, G. Chandra Praba, K. Abhirami and S. Puvaneswari, "BLOCKCHAIN BASED CERTIFICATE VALIDATION SYSTEM," *International Research Journal of Modernization in Engineering Technology and Science* , vol. 04, no. 07, 2022.

[5] "IBM," [Online]. Available: https://www.investopedia.com/terms/b/blockchain.asp.

[6] "Dune," [Online]. Available: https://docs.dune.com/data-catalog/evm/sepolia/overview.

[7] "IBM," [Online]. Available: https://www.ibm.com/think/topics/smart-contracts.

[8] "GeeksforGeeks," [Online]. Available: https://www.geeksforgeeks.org/introduction-to-solidity/.

[9] "IPFS| Docs," [Online]. Available: https://docs.ipfs.tech/concepts/what-is-ipfs/.

[10] "GeeksforGeeks," [Online]. Available: https://www.geeksforgeeks.org/sha-256-and-sha-3/.

[11] "CoinMarketCap," [Online]. Available: https://coinmarketcap.com/academy/article/what-is-metamask.
[12] "GeeksforGeeks," [Online]. Available: https://www.geeksforgeeks.org/reactjs-introduction/.