A Decentralized Approach to Academic Certificate Management Using Blockchain and IPFS

Dr. Harika B[1], Ch. Sidhardha[2], K. Manikanta[3]
[1] *Associate Professor, Mahatma Gandhi Institute of Technology*
[2,3] *UG Student, Mahatma Gandhi Institute of Technology*

Abstract- **The increasing incidence of forged academic certificates has necessitated the development of secure, verifiable systems for credential management. This research proposes a decentralized approach to academic certificate issuance, storage, sharing, and verification utilizing blockchain technology and the InterPlanetary File System (IPFS). The system leverages blockchain's immutability to ensure trust and transparency, while IPFS provides decentralized and tamper-proof certificate storage. Advanced cryptographic techniques, including Elliptic Curve Cryptography (ECC) and AES encryption, are incorporated to enhance data confidentiality during storage and transmission. Smart contracts deployed on the blockchain handle the logging and validation of certificate records, enabling seamless and trustless verification. The proposed system demonstrates a significant improvement over traditional centralized models by providing enhanced security, transparency, and resistance to document tampering. Experimental results validate the effectiveness and efficiency of the system, highlighting its potential as a reliable solution for academic institutions and verifiers worldwide.**

Keywords: **Blockchain, Cryptography, SHA-256 hashing, Elliptic Curve Cryptography (ECC), AES encryption, Privacy, Tampering resistance, Forgery prevention, Operational efficiency, Smart Contracts, IPFS, Decentralised Storage.**

I. INTRODUCTION

The growing prevalence of fraudulent academic certificates poses a significant threat to educational institutions, employers, and students alike. Traditional certificate issuance and verification systems are centralized, making them vulnerable to manipulation, data breaches, and administrative inefficiencies. As a result, there is a pressing need for a secure, transparent, and tamper-proof method to manage academic credentials. Blockchain technology offers a decentralized solution that ensures immutability and verifiability of data, while the InterPlanetary File System (IPFS) provides distributed storage that is resistant to data loss and unauthorized alteration. This research explores the integration of blockchain and IPFS for academic certificate management, focusing on secure issuance, encrypted storage, verifiable sharing, and real-time validation using smart contracts and cryptographic techniques such as Elliptic Curve Cryptography (ECC) and AES encryption.

A. Problem Statement.

Traditional academic certificate systems face persistent challenges such as forgery, data tampering, and inefficient verification processes, which significantly undermine the credibility and trustworthiness of educational credentials. These systems, often reliant on centralized infrastructure, are susceptible to data breaches, manual errors, procedural delays, and high administrative costs—factors that hinder smooth and secure certificate management. With the rapid growth of online education and global mobility, there is a rising demand for certificate systems that are secure, scalable, and transparent. Existing mechanisms struggle to meet these modern requirements, often relying on outdated practices that are ill-suited to a digital-first environment. As a result, students, employers, and academic institutions alike face difficulties in verifying qualifications promptly and reliably.

To address these issues, there is a growing need for decentralized, tamper-resistant solutions that ensure the authenticity, integrity, and accessibility of academic records. This project proposes a blockchain-based framework designed to provide a secure, efficient, and privacy-compliant system for the issuance, storage, and verification of academic certificates. By harnessing cryptographic techniques and distributed ledger technology, the system aims to enhance trust, reduce verification overhead, and streamline credential management on a global scale.

B. Existing System

In recent years, several blockchain-based solutions have been proposed to improve the security, transparency, and efficiency of academic certificate issuance and verification. One of the most commonly adopted approaches utilizes the Ethereum blockchain, where cryptographic hashes of certificates are stored using smart contracts in conjunction with SHA-256 hashing. This ensures immutability of records and facilitates public, tamper-resistant verification mechanisms. Alternatively, solutions based on Hyperledger Fabric—a permissioned blockchain—offer a more controlled environment with fine-grained access management. These systems are well-suited for consortiums of educational institutions, allowing authorized members to securely define

access rules, manage data collaboratively, and preserve privacy.

To address on-chain storage limitations, many systems integrate the InterPlanetary File System (IPFS), a decentralized file storage network. With this approach, certificate documents are stored off-chain in IPFS, while only their cryptographic hashes or references are recorded on the blockchain. This significantly reduces transaction costs and enhances scalability without compromising integrity or verifiability. Additionally, some advanced implementations tokenize academic certificates using the ERC-721 standard, transforming them into non-fungible tokens (NFTs). This enables unique ownership, secure transfer, and on-chain authenticity tracking.

Many modern platforms also employ smart contract-based verification, wherein the logic for validating certificates is embedded directly into the contracts. These smart contracts autonomously execute validation rules, eliminating intermediaries and reducing the risk of human error or fraud. However, existing systems face several limitations. Public blockchains like Ethereum are often burdened with high transaction fees and scalability issues due to network congestion. Furthermore, systems built on Proof of Work (PoW) consensus models can suffer from slow processing times and excessive energy consumption. Some platforms lack robust encryption or proper key management, exposing data to tampering and unauthorized access. Despite using blockchain, a few implementations still require manual blockchain queries for verification, reducing overall efficiency and automation.

II. LITERATURE SURVEY

The paper examines the challenges posed by European data protection regulations in designing software systems for managing personal data. It studies blockchain and off-chain technologies to assess their strengths and weaknesses concerning regulatory compliance. Since blockchain's intrinsic characteristics conflict with data protection laws, the study incorporates off-chain constructs to address these limitations. The proposed framework adopts a hybrid approach, utilizing blockchain for access control, audit, and integrity verification while storing personal data off-chain. The methodology includes system architecture design, use case modeling, and a security and privacy threat analysis, demonstrated through a digital academic certificates system. While the framework addresses key challenges, further research is needed to enhance threat mitigation and decentralized actor authentication. [1]

The study presents QualiChain, a blockchain-based platform designed for smart badge accreditation in higher education. The platform integrates data analytics, decision support tools, and blockchain technology within a layered architecture to manage credentials, validate qualifications, and provide personalized educational services. By leveraging Ethereum's blockchain with ERC721 tokens, the system ensures the immutability and verifiability of smart badges. Semantic Web technologies and the OpenBadges standard embed machine-readable qualifications in user profiles. Key methods include the Elliptic Curve Digital Signature Algorithm (ECDSA) for secure transactions, Multi-Criteria Decision Support Systems (MCDSS) for course recommendations, knowledge graphs for ontology-based data storage, and smart contracts for automated accreditation. Piloted with over 100 students and professors at the National Technical University of Athens, the platform demonstrates potential in streamlining credential management but highlights the need for improved scalability, user-interface design, and institutional integration. The findings underscore blockchain's role in enhancing trust, transparency, and decentralized validation mechanisms in education. [2]

The research proposes a blockchain-based system for secure and efficient certificate validation. The system allows educational institutions to register, upload scanned certificates, and generate unique hash values using the SHA-256 algorithm. These hashes, stored on a blockchain, ensure tamper-proof and transparent recordkeeping. Certificates are validated through a user-friendly portal, where stakeholders (students or organizations) input unique IDs or credentials to confirm authenticity. The system employs the Proof of Work (PoW) consensus algorithm to securely add blocks to the blockchain. This approach eliminates forgery and manual inefficiencies in certificate verification, offering a secure, decentralized, and accessible digital storage solution. The advantages include reduced risks of fake certificates, transparency, and traceability, but challenges such as high computational costs, scalability concerns, and the need for internet access and technical expertise remain. By integrating smart contracts and cryptographic algorithms, the method provides a reliable alternative to traditional certificate management. [3]

The study introduces a blockchain-based system to enhance the authentication and privacy of university certificates using smart contracts. The system utilizes a SHA-256 hashing algorithm to generate unique hashes for certificates, which are stored on the blockchain to ensure tamper-proof integrity. It features a modular web application with three main components: a Request Certificate Module for students to submit requests, an Approve Certificate Module for university administrators to verify and approve these requests, and a Verify Certificate Module that allows third parties to validate certificates by comparing hashes. Smart contracts manage interactions, ensuring that only authorized personnel can add

or retrieve certificate hashes, streamlining the certificate generation process while enhancing trust in academic credentials. The findings highlight the potential of blockchain technology to transform certificate management in educational institutions. [4]

The paper proposes an innovative blockchain-based model aimed at enhancing the management of academic records in the education sector. It addresses critical challenges such as scalability, privacy, and compliance with regulations like the General Data Protection Regulation (GDPR). By utilizing smart contracts within a consortium blockchain framework, the proposed system facilitates the secure issuance, storage, and verification of both formal and informal academic information. The model allows holders to authorize third parties to access their records while ensuring the protection of personal data. Additionally, it includes mechanisms for modifying or deleting academic information and provides a solution for recovering records if an educational institution ceases to exist, leveraging distributed file systems like IPFS. Implemented as a proof of concept using Hyperledger Fabric, a type of private blockchain, the framework demonstrates a scalable and privacy-compliant approach to managing educational data, paving the way for future developments and real-world validation. [5]

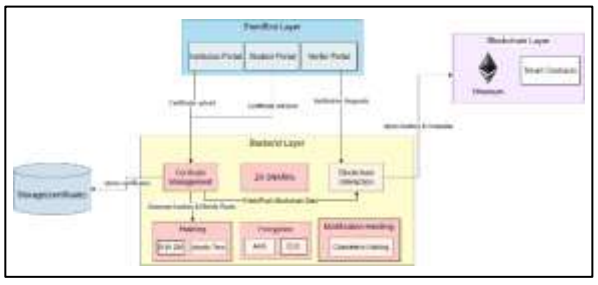
The study presents a blockchain-based system for certificate verification and transcript generation to combat forgery, inefficiency, and document loss. The system issues certificates that are hashed for authenticity and stored using Ethereum blockchain and IPFS, ensuring secure and tamper-proof records. Smart contracts automate certificate issuance and validation, reducing manual work and errors. Users, including students and organizations, can verify certificates via unique hash, enabling quick and reliable validation. The system also provides role-based access, allowing certificate issuers, students, and validators to interact securely. The integration of Ethereum tools like Solidity, Ganache for testing, and MetaMask for payment approvals enhances security and functionality. Distributed storage via IPFS mitigates risks of centralized failure, while Ethash ensures efficient proof-of-work. The findings suggest that the system eliminates risks associated with physical certificates, such as loss or damage, and offers a transparent, scalable solution for document management. [6]

The research introduces HEDU-Ledger, a blockchain-based system designed for secure degree attestation and verification by the Higher Education Commission (HEC). Utilizing Hyperledger Fabric, the system creates a decentralized, private, and permissioned blockchain network to ensure the immutability and traceability of academic credentials. Smart contracts automate processes such as credential validation, attestation, and traceability, while external storage systems like IPFS securely store associated documents. The system connects stakeholders, including universities, government bodies, and employers, through a peer-to-peer network, offering efficient, tamper-proof verification. By replacing manual and semi-automated processes with a blockchain-enabled solution, the system addresses issues like forgery, inefficiency, and high administrative costs. However, challenges include scalability, cross-platform adoption, and implementation costs. The study suggests that HEDU-Ledger enhances security, transparency, and efficiency in managing academic credentials while minimizing fraudulent activities and administrative overhead. [7]

III. PROPOSED MODEL

The proposed model presents a decentralized, secure, and transparent system for managing student academic certificates using blockchain and hybrid encryption. It involves three primary actors—Institutions, Students, and Verifiers—each interacting through a web-based interface backed by smart contracts and IPFS. Institutions issue certificates that are encrypted using AES, and the AES key itself is encrypted using ECC with the student's public key. These encrypted certificates are stored on IPFS, while the corresponding hash and digital signature are logged immutably on the Ethereum blockchain. Students can later decrypt their certificates or selectively share them by re-encrypting the AES key with a verifier's public key. Verifiers can access the shared data, verify its integrity through hash comparison, and confirm authenticity via the blockchain-stored digital signature.

A. *Architecture of Proposed Model*



The system architecture is designed with four key layers: Frontend, Backend, Blockchain, and Storage, each serving a distinct purpose to ensure efficient, secure, and scalable certificate management and verification. The Frontend Layer provides user interfaces for different actors, with dedicated portals for institutions, students, and verifiers. Institutions can issue certificates, students can retrieve, view, and share their certificates securely, while verifiers can authenticate the

certificates shared with them. The Backend Layer is the processing engine of the system, handling critical tasks like certificate management, cryptographic operations, and interaction with the blockchain. It uses AES encryption to secure certificates and ECC for secure key exchanges, ensuring that only authorized users can access or share certificates. The Blockchain Layer provides immutability and transparency by storing the hash values of certificates and metadata on the Ethereum blockchain, specifically on the Sepolia testnet. Smart contracts automate the process of storing and verifying certificate hashes, enabling efficient and trustworthy validation of certificates. Finally, the Storage Layer employs IPFS for decentralized storage of full certificates, ensuring they remain secure and tamper-proof. MongoDB stores certificate metadata, such as student information and certificate IDs, allowing for quick access and efficient management of the certificate records. This layered architecture ensures a robust, secure, and efficient system for managing and verifying blockchain-based certificates.

IV. METHODOLOGY

This methodology leverages blockchain and cryptographic techniques to ensure the security and authenticity of student certificates. MetaMask authentication is used for user verification. AES encryption secures certificates, while ECC generates digital signatures for authenticity. Certificates are stored on IPFS for immutability, and blockchain-based verification ensures transparent and tamper-proof certificate validation.

A. User Authentication using MetaMask

User authentication is a critical aspect of ensuring that only authorized individuals can interact with the certificate issuance and verification system. In this project, MetaMask, a popular cryptocurrency wallet and browser extension, is employed for user authentication. MetaMask enables secure login via Ethereum-based credentials, allowing institutions, students, and verifiers to authenticate their identities through their MetaMask wallet. By connecting their wallet to the platform, users can sign transactions securely, and their identities are verified using their public Ethereum address.

B. Encryption Using the AES Approach

The Advanced Encryption Standard (AES) is a symmetric block cipher widely adopted as a standard for securing sensitive data. Developed to replace the aging Data Encryption Standard (DES), AES offers significantly enhanced security and efficiency. Its symmetric nature implies that the same secret key is used for both encryption and decryption processes.

Steps in AES Encryption:

i. SubBytes: This operation relies on a substitution box (S-box), denoted as S(byte). For each byte bij in the state matrix A, the output byte bij' is given by:

$$bij' = S(bij)$$

The S-box itself is a fixed 16x16 lookup table derived from mathematical principles involving multiplicative inverses in $GF(2^8)$ and an affine transformation.

ii. ShiftRows: This operation involves a cyclic left shift of the rows of the state matrix. For a state matrix A where Ai,j represents the byte in row i and column j (with i ranging from 0 to 3), the shifted state A′ has rows shifted as follows: $A'_{0,j} = A_{0,j}$

$$A'_{1,j} = A_1, (j+1) mod 4$$
$$A'_{2,j} = A_2, (j+2) mod 4$$
$$A'_{3,j} = A_3, (j+3) mod 4$$

iii. MixColumns: This operation treats each column of the state as a four-term polynomial over GF(28) and multiplies it by a fixed polynomial
$a(x) = \{03\}x^3 + \{01\}x^2 + \{01\}x + \{02\}\ modulo\ x^4 + 1$. If a column is represented as s(x)=s3x3+s2x2+s1x+s0, the resulting column $s'(x) is$:

$$s'(x) = a(x) \cdot s(x) (mod x^4 + 1)$$

This multiplication involves specific rules of polynomial multiplication within $GF(2^8)$. For a column vector

$$S = [s_0, s_1, s_2, s_3]^T,$$

the operation can be represented as a matrix multiplication with a fixed 4×4 matrix

$$M: S' = M \cdot S$$

Iv. AddRoundKey: This is a bitwise XOR operation between the current state and the round key $K(r)$:

$$State^{(r+1)} = State^{(r)} \oplus K^{(r)}$$

where $\oplus$ denotes the bitwise XOR operation.

Repeat Rounds (Rounds 2 to 9)

Perform 9 more rounds (with proper round keys from expanded key schedule). The final round skips the MixColumns step. Then the encrypted cipher text is produced. And for Decryption the process same as Encryption but in reverse.

C. Digital Signature Generation using ECC

Elliptic Curve Cryptography (ECC) is a form of public key cryptography based on the algebraic structure of elliptic curves over finite fields. ECC offers the same level of security as RSA but with much smaller key sizes, making it more efficient.

The process of generating a digital signature using ECC involves the following steps:

i. **Key Generation:** A private key *d* is randomly selected from the set of integers modulo the order nnn of the elliptic curve. A public key *Q* is computed by multiplying the generator point PPP of the elliptic curve by the private key *d*:

$$Q = dP$$

ii. Hashing the Message: The message *M* to be signed is hashed using a cryptographic hash function (e.g., SHA-256), producing a hash *H(M)*.

iii. **Signature Generation**: A random integer *k* is selected. This *k* is used to compute the signature components:

$$r = (kP)_x t mod n$$
$$s = k-1(H(M)+rd) mod n$$

The signature *(r,s)* is sent along with the message.

The security of the digital signature relies on the difficulty of solving the Elliptic Curve Discrete Logarithm Problem (ECDLP). The private key ddd remains secure, even if the public key QQQ and signature are known.

D. Certificate Creation and Encryption

The issuance of a certificate in a blockchain-based system begins with the creation of a digital certificate that authenticates a student's achievements. The institution generates the certificate, which is then encrypted using the Advanced Encryption Standard (AES) for confidentiality. Once encrypted, the certificate is signed using Elliptic Curve Cryptography (ECC) to ensure authenticity and prevent tampering. The certificate, along with its digital signature, is stored on the blockchain, ensuring immutability. Additionally, the certificate is stored off-chain on the InterPlanetary File System (IPFS), with its IPFS hash recorded on the blockchain to link it to decentralized storage.

E. Secure Certificate Sharing

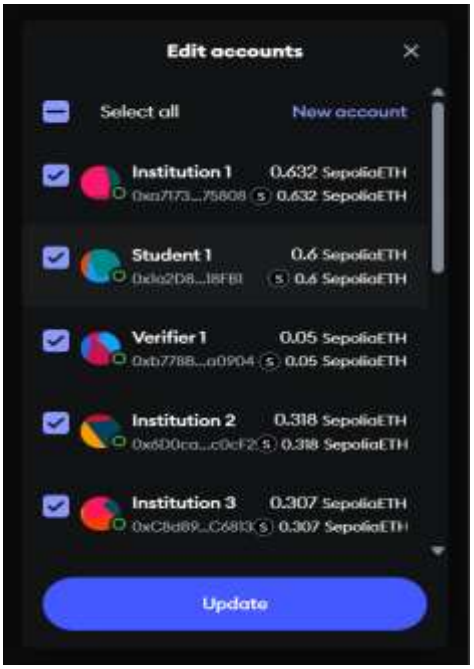
When a student shares their certificate with a verifier, the certificate, encrypted with AES, is first decrypted using the student's private key. Then, the AES key is re-encrypted with the verifier's public key, ensuring that only the verifier can decrypt the certificate. The student sends both the encrypted certificate and re-encrypted AES key to the verifier, who uses the blockchain and ECC-based digital signatures to verify the certificate's authenticity. This process ensures the certificate's security throughout sharing and verification, leveraging AES for encryption, ECC for key exchange, and blockchain for secure record-keeping.

F. Blockchain-Based Certificate Verification

Once shared, the verifier uses the blockchain to verify the certificate's authenticity. This verification process leverages the blockchain's decentralized nature, making it transparent, traceable, and tamper-resistant. The certificate's digital signature and metadata are recorded on the blockchain, ensuring any alterations will be detected. Verifiers compare the certificate's hash with the one stored on the blockchain to ensure integrity. Blockchain's distributed ledger system guarantees a secure, transparent, and trustworthy solution for certificate verification across various domains.

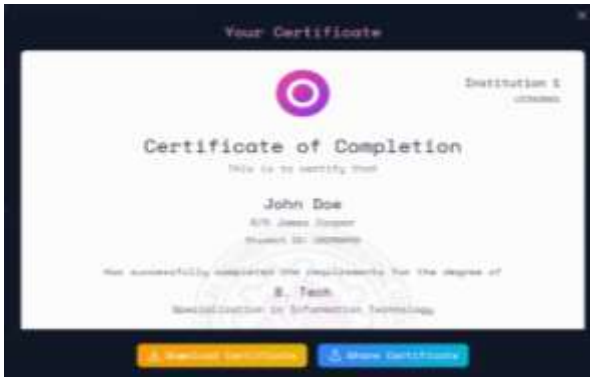
IV. RESULT ANALYSIS

The implementation was successfully deployed and tested on the Ethereum Sepolia testnet using multiple role-specific accounts, as shown in the MetaMask wallet interface. Each account corresponds to a distinct user role within the system—Institutions, Students, and Verifiers. During testing, certificates were issued by institution accounts (e.g., Institution 1 with 0.632 SepoliaETH), received and managed by student accounts (e.g., Student 1 with 0.6 SepoliaETH), and later verified by verifier accounts (e.g., Verifier 1 with 0.05 SepoliaETH). The allocation of SepoliaETH across these accounts confirmed successful execution of transactions including smart contract interactions, certificate issuance, and verification. These results validate the feasibility of role-based operations and transaction integrity on the Ethereum network, ensuring a secure and functional end-to-end workflow.

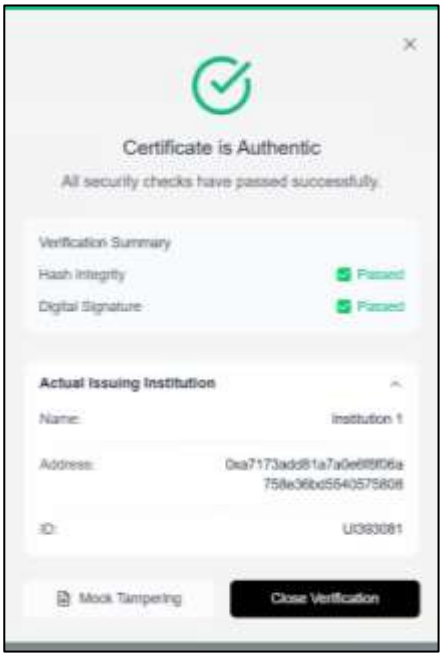


The below image displays the detailed transaction information related to the certificate issuance recorded on the Ethereum blockchain (Sepolia testnet). It provides important details such as the transaction hash, block number, block status, gas fees, and the exact timestamp when the transaction was confirmed. These elements are crucial for verifying the successful execution of the smart contract that logs the certificate's hash, metadata, and digital signature. By examining this transaction, one can assess the gas consumption associated with storing certificate-related data on the blockchain, ensuring transparency and traceability of the process. The image showcases the immutability and auditability provided by the blockchain, where every transaction is securely recorded and can be independently verified.

When the user clicks on one of the certificate cards, it displays the decrypted certificate. The image shows a detailed certificate of completion awarded to a student, along with options to securely download or share the certificate. On the backend, the encrypted certificate is retrieved from IPFS using the stored hash, and the AES key is decrypted using the student's private key. Once decrypted, the certificate is displayed in a structured format on the frontend. For sharing, the AES key is re-encrypted with the verifier's public key, ensuring secure transmission. The backend ensures that only authorized users can access the certificate, maintaining confidentiality and integrity throughout the process..



The certificate verification process begins by retrieving the certificate's hash, metadata, and digital signature from the blockchain, ensuring its immutability and integrity. The encrypted certificate is fetched from IPFS, and the backend decrypts it using the verifier's private key, granting access to the certificate's full details. Once decrypted, the digital signature is verified using Elliptic Curve Cryptography (ECC), confirming the certificate's authenticity. This process, enabled by the secure backend, ensures real-time, automated, and tamper-proof certificate verification, leveraging blockchain for transparent and fraud-resistant validation.



To assess the performance of the blockchain-based certificate system, key metrics were measured across its workflow. AES encryption averaged 25 ms per certificate, while ECC signing took about 40 ms. Uploading to IPFS averaged 1.2 seconds, mainly due to network latency. Blockchain transactions on the Sepolia testnet required 20–25 seconds, reflecting standard block confirmation delays. On the verifier's side, decryption and verification were completed in roughly 100 ms, confirming the system's suitability for near real-time verification..

Operation	Average Time Taken
AES Encryption	~25 ms
ECC Digital Signing	~40 ms
Upload to IPFS	~1.2 s
Blockchain Transaction (Sepolia)	~10–15 s
Certificate Decryption & Verification	~100 ms

The system uses blockchain transactions on the Sepolia testnet to log certificate metadata, IPFS hashes, and digital signatures. Issuance transactions consumed around 130,000–150,000 gas units, costing approximately 0.0015 to 0.002 ETH. Since certificate verification reads existing on-chain data, it incurs minimal or no gas fees. By limiting write operations and optimizing transactions, the system maintains cost-efficiency and scalability.

Operation	Certificate Issuance (Write Tx)
Average Gas Used	45,000–60,000
Estimated Cost (ETH)	0.0011–0.0013 ETH
Remarks	₹190–₹230 (approx.)

The blockchain-based system outperforms traditional certificate issuance by using decentralized storage (IPFS and blockchain) and automated smart contract verification. Unlike manual verification and signature stamps in traditional systems, blockchain ensures tamper resistance, ECC digital signature authentication, and AES-encrypted sharing. Additionally, it offers stronger access control and full transparency, unlike traditional systems' opaque processes.

V. CONCLUSION

The Blockchain-Based Student Certificate Verification System addresses critical issues in traditional certificate management, such as forgery, inefficiency, and reliance on centralized authorities. By leveraging blockchain technology, the system ensures transparency, immutability, and enhanced security for certificate issuance and verification. It integrates cryptographic techniques like SHA-256, AES encryption, and Zero-Knowledge Proofs (ZK-SNARKs) to create a tamper-proof and privacy-preserving framework. With its decentralized architecture, certificates are securely stored and verified through blockchain, eliminating the risks of data tampering or single points of failure. The user-centric design includes dedicated portals for institutions, students, and verifiers, ensuring seamless interaction and streamlined workflows. Off-chain storage solutions like IPFS and real-time blockchain integration enhance scalability while reducing costs. Advanced cryptographic methods ensure that the system upholds security and privacy standards without compromising efficiency. Overall, this project demonstrates how blockchain can revolutionize academic certificate management by providing a secure, scalable, and trustworthy solution. It not only safeguards the authenticity of credentials but also builds trust among stakeholders, paving the way for broader adoption of blockchain-based systems in education and beyond.

REFERENCES

[1] F. Molina, G. Betarte, and C. Luna, "*A Blockchain-based and GDPR-compliant design of a system for digital education certificates*," CLEI Electron. J., vol. 26, May 2023.

[2] C. Kontzinos, E. Karakolis, P. Kokkinakos, S. Skalidakis, D. Askounis, and J. Psarras, "*Application and Evaluation of a Blockchain-Centric Platform for Smart Badge Accreditation in Higher Education Institutions*," Appl. Sci., 2024.

[3] M. Suganthalakshmi, G. Chandra Praba, K. Abhirami, and S. Puvaneswari, "*Blockchain based certificate validation system*," International Research Journal of Modernization in Engineering Technology and Science, 2022.

[4] G. H. Lokesh, U. M. V V Nalagath and F. Flammini, "*Providing authentication and privacy for university certificates using smart contracts in blockchain technology*," Interdisciplinary Description of Complex Systems, vol. 20, no. 4, pp. 398-412, 2022.

[5] C. Delgado-von-Eitzen, L. Anido-Rifón, and M. J. Fernández-Iglesias, "*Application of Blockchain in Education: GDPR-Compliant and Scalable Certification and Verification of Academic Information,"* Appl. Sci., vol. 11, 2021.

[6] R. S. Lamkoti, D. Maji, B. Gondhalekar, and H. Shetty, "*Certificate verification using blockchain and generation of transcript*," International Journal of Engineering Research & Technology (IJERT), vol. 10, no. 3, 2021.

[7] A. A. Ayub Khan, A. A. Laghari, A. A. Shaikh, S. Bourouis, A. M. Mamlouk, and H. Alshazly, "*Educational Blockchain: A Secure Degree Attestation and Verification Traceability Architecture for Higher Education Commission*," Appl. Sci., vol. 11, no. 10917, 2021.