International Journal of Engineering Research and Science & Technology

www.ijerst.org

ISSN : 2319-5991

Vol. 22 No. 2 (2026)

ijerst.editor@gmail.com

editor@ijerst.com

International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com
Vol. 22, No. 2, 2026

Peer Reviewed, Referred & Indexed Journal

A Faster, Integrated, and Trusted Certificate Authentication and Issuer Validation System Based on Blockchain

1.C.Manjusha,Asst.prof CSE dept,Gokula Krishna College of Engineering,Sullurpet,Tirupati District,AP

2.B.Chandra Harsha, P.Vamsi Krishna, D.Sai Kiran, E.Chandrakala, P.Apuroopa, CSE dept,Gokula Krishna College of Engineering,Sullurpet,Tirupathi District,AP.

ABSTRACT

The rapid growth of digital education and online recruitment has increased the need for secure and reliable certificate verification systems. Conventional certificate validation methods rely on centralized databases or manual verification processes, which are slow, vulnerable to tampering, and prone to single points of failure. To address these limitations, this study proposes an enhanced blockchain-based framework for certificate authentication and issuer validation that ensures transparency, security, and operational efficiency. The proposed mechanism integrates decentralized blockchain architecture with cryptographic hashing and smart contracts to securely record certificate information in an immutable ledger. Each certificate is transformed into a unique cryptographic hash, which is stored on the blockchain to prevent unauthorized modifications and guarantee data integrity. A consortium-based validation model is introduced in which trusted institutions collectively verify and authorize new certificate issuers through a voting mechanism, strengthening system reliability. In addition, a Bloom Filter-based search optimization technique is incorporated to significantly reduce certificate lookup time during verification requests. This approach minimizes unnecessary blockchain queries, improving overall system performance and scalability. Experimental analysis demonstrates that the proposed architecture reduces verification time, enhances security against fraudulent certificates, and lowers operational costs compared with traditional systems. The developed framework provides a scalable, transparent, and tamper-resistant platform suitable for academic institutions, recruitment agencies, and government organizations requiring trustworthy digital certificate management.

Keywords— Blockchain, certificate verification, authentication, Ethereum, smart contracts, Bloom filter, decentralized system, hash function, digital certificates, search optimization.

I. INTRODUCTION

The rapid digitalization of education and recruitment systems has significantly increased the importance of secure certificate verification mechanisms. Educational institutions issue millions of academic certificates every year, and these documents are frequently used for employment, higher education, and professional licensing. However, traditional certificate verification approaches rely on manual checking procedures or centralized databases maintained by institutions, which are often inefficient, time-consuming, and susceptible to fraud. As digital documentation becomes widespread, the risk of forged or manipulated certificates has increased considerably, creating serious challenges for organizations that depend on accurate credential validation [1], [2].

Conventional verification systems typically depend on centralized authorities that manage certificate records. While these systems provide some level of control, they introduce several limitations such as single points of failure, lack of transparency, and vulnerability to cyberattacks. If the centralized database is compromised or becomes unavailable, the entire verification infrastructure may collapse. Furthermore, centralized architectures make it difficult for third-party organizations to independently verify certificate authenticity without direct interaction with the issuing authority, resulting in delays and increased operational overhead [3]. The growing number of phishing attacks and credential compromises has further emphasized the need for more reliable and tamper-resistant certificate management systems [1].

Blockchain technology has emerged as a promising solution for addressing these challenges due to its decentralized architecture, immutability, and transparency. A blockchain is a distributed ledger that records transactions across multiple nodes in a network, ensuring that stored information cannot be altered without consensus among participants. Once data is recorded in a blockchain, it becomes permanent and verifiable, making the technology highly suitable for applications requiring trust and integrity, such as digital credential management

[4], [5]. Smart contracts further enhance blockchain capabilities by enabling automated execution of predefined rules without requiring intermediaries, thereby improving efficiency and reducing operational complexity [6].

Several researchers have explored the use of blockchain for secure certificate verification and credential management. Blockchain-based systems can store certificate data in encrypted or hashed form, allowing organizations to verify authenticity without exposing sensitive information [7]. Such systems eliminate the dependency on centralized authorities and enable transparent verification processes across multiple stakeholders. Furthermore, distributed verification frameworks can significantly reduce the time required for credential validation while improving reliability and auditability [8], [9].

Despite these advancements, existing blockchain-based certificate verification systems still face several challenges, including inefficient search mechanisms, high transaction costs, and limited scalability when handling large volumes of certificates. Many systems store certificate records directly on blockchain networks without incorporating efficient indexing or search optimization techniques, which can result in increased verification latency during large-scale operations [10]. Moreover, some proposed solutions rely on centralized storage components or limited validator participation, which reduces the advantages offered by decentralized architectures [11], [12].

To address these limitations, this study proposes a faster, integrated, and trusted certificate authentication and issuer validation system based on blockchain technology. The proposed framework leverages decentralized blockchain infrastructure combined with cryptographic hashing and smart contracts to ensure secure certificate storage and verification. A consortium of trusted institutions participates in the validation of certificate issuers through a voting mechanism, which enhances the reliability of the system and prevents unauthorized entities from issuing certificates. In addition, a Bloom Filter-based search optimization technique is integrated to significantly reduce certificate lookup time during verification processes. This optimization improves performance by minimizing unnecessary blockchain queries and enabling faster detection of invalid certificates.

The proposed architecture ensures that certificates remain tamper-proof, transparent, and easily verifiable while maintaining privacy through cryptographic hashing. By combining decentralized validation mechanisms with efficient search optimization, the system provides a scalable and cost-effective solution for digital certificate authentication. The framework can be applied in academic institutions, recruitment systems, professional certification bodies, and government organizations that require secure and trustworthy credential verification.

II. LITERATURE SURVEY

Blockchain technology has gained significant attention in recent years as a reliable approach for secure data management and decentralized authentication systems. Researchers have explored its potential in various domains including healthcare, supply chain management, digital identity verification, and academic credential validation. In the context of certificate authentication, blockchain provides an immutable and transparent environment that prevents unauthorized modification of records while enabling efficient verification processes [4], [5].

Several studies have proposed blockchain-based frameworks for managing digital certificates and credentials. Pericàs-Gornals et al. introduced a privacy-preserving blockchain system for managing digital COVID-19 certificates, where proxy re-encryption techniques were used to enhance data privacy and security [11]. Although the system provided secure certificate validation, its design was specifically tailored for healthcare applications and lacked flexibility for broader academic credential verification scenarios.

Mondal et al. proposed an efficient blockchain-based e-certificate management system in which certificates are stored using cryptographic techniques and verified through distributed ledger technology [12]. The system eliminates the need for intermediaries and ensures data integrity through cryptographic encryption methods such as elliptic curve cryptography. However, the framework did not focus on optimizing certificate search mechanisms, which can significantly affect performance when verifying large numbers of certificates.

Zhang et al. presented a hybrid blockchain architecture for authentication of heterogeneous IoT nodes using trust-based mechanisms and blockchain integration [13]. While their work demonstrated the potential of blockchain for secure authentication in IoT environments, the approach primarily focused on device authentication rather than academic certificate validation. Similarly, Nguyen et al. explored blockchain-based decentralized applications and proposed design considerations for integrating blockchain with authentication systems [14]. Their research provided valuable insights into blockchain architecture and interoperability, but it did not provide a complete solution for certificate management and issuer validation.

Elloh Adja et al. proposed a blockchain-based certificate revocation and status verification system to address limitations of traditional public key infrastructure. Their framework used blockchain to maintain a decentralized list of certificate authorities and revocation information [15]. Although the system improved transparency and reliability, it was not designed specifically for academic credential verification and did not include mechanisms for optimizing verification time.

Merlec et al. introduced a consortium blockchain model for secure electronic portfolio management where academic records are stored on a blockchain network [16]. The framework ensured secure storage and verification of

educational credentials; however, its flexibility and scalability for large-scale institutional networks were limited. Garba et al. proposed LightLedger, a blockchain-based domain certificate authentication scheme that incorporated zero-knowledge proofs to enhance privacy and security [17]. While the system improved certificate authority management, the validator selection process remained random, which could potentially affect reliability in institutional verification systems.

Rahman et al. developed a blockchain-based certificate authentication framework with correction mechanisms that allow universities to update previously issued certificates when errors occur [18]. Their architecture used a dual-chain structure to separate certificate storage and correction records. Although this design improved certificate management, it was limited to a single institutional network and lacked a robust multi-institution validation mechanism.

Killedar et al. proposed a blockchain-based academic certificate authentication platform with a user-friendly decentralized application interface for both administrators and students [19]. The system simplified certificate issuance and verification processes; however, it introduced additional operational costs and did not include a dedicated validation authority mechanism. Similarly, Rahardja et al. developed a blockchain-enabled digital certificate authentication framework that ensures global accessibility and tamper-proof storage of academic records [20]. Although their approach improved accessibility, it relied on partially centralized storage components that could introduce vulnerabilities.

From the existing literature, it can be observed that blockchain provides strong security features for certificate verification, including immutability, transparency, and decentralized trust mechanisms. However, many existing systems suffer from limitations such as inefficient search processes, restricted validator participation, and lack of scalable verification frameworks. These limitations highlight the need for an improved blockchain-based certificate authentication system that integrates efficient search optimization, decentralized issuer validation, and cost-effective transaction mechanisms.

The proposed system addresses these challenges by combining blockchain technology with hash-based certificate storage, consortium-based issuer validation, and Bloom Filter-based search optimization. This integrated approach significantly improves verification speed while maintaining strong security and trust mechanisms.

III. PROPOSED METHODOLOGY

The proposed system introduces a secure and decentralized certificate authentication and issuer validation framework using blockchain technology. The objective of the methodology is to ensure tamper-proof certificate storage, trusted issuer validation, fast certificate verification, and privacy preservation. The system integrates blockchain infrastructure, smart contracts, cryptographic hashing, Bloom Filter optimization, and consortium-based validation to provide an efficient and scalable verification platform.

The architecture is designed to eliminate the weaknesses of traditional centralized verification systems by distributing trust among multiple participating institutions. Each certificate transaction is securely recorded on the blockchain, ensuring transparency, immutability, and auditability.

3.1 System Architecture

The proposed architecture consists of four major entities:

1. Trusted Validators
2. Certificate Issuers
3. Certificate Holders
4. Verification Clients

Each entity performs a specific function in the certificate authentication lifecycle.

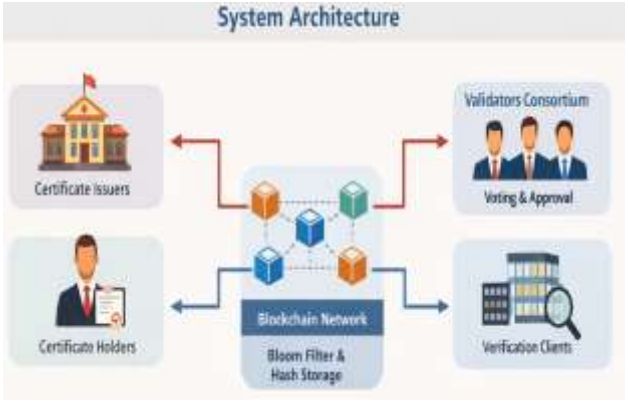

Figure.1: Proposed Architecture

The architecture illustrates the interaction between certificate issuers, validators, certificate holders, and verification clients within a decentralized blockchain network that securely stores certificate hashes. Bloom Filter optimization and smart contracts enable faster verification while validators maintain system trust through consensus-based issuer approval.

1. Validators

Validators are trusted institutions responsible for maintaining the blockchain network and validating transactions. They verify the authenticity of certificate issuers through a consensus-based voting mechanism.

2. Certificate Issuers

Authorized institutions generate and issue certificates. Before issuing certificates, institutions must be validated by the consortium of validators.

3. Certificate Holders

Certificate holders are individuals who receive certificates issued by trusted institutions.

4. Verifiers

Organizations such as employers, universities, or government bodies verify certificate authenticity through the blockchain network.

The overall workflow involves issuer validation, certificate generation, certificate storage, and verification processes.

3.2 Blockchain-Based Certificate Storage

The proposed system uses blockchain as a distributed ledger to store certificate information in the form of cryptographic hashes. Instead of storing the entire certificate data, only the hash representation of the certificate is stored on-chain to ensure data privacy and reduce transaction size.

Let the certificate data be represented as:

$$C = \{Name, ID, Course, Institution, Year\}$$

A cryptographic hash function

$H(\cdot)$ is applied to generate a unique certificate fingerprint.

$$CH = H(C)$$

Where:

CH = Certificate Hash

H= Secure Hash Algorithm (SHA-256)

SHA-256 generates a 256-bit fixed-length output.

$$CH = SH\ A256(C)$$

The generated hash is stored on the blockchain through a smart contract transaction.

This mechanism ensures:

- Immutability
- Integrity verification
- Efficient storage

If any modification occurs in the certificate data, the hash changes completely, allowing easy detection of tampering.

3.3 Smart Contract-Based Certificate Management

Smart contracts automate certificate issuance, validation, and verification operations.

The smart contract includes the following functions:

1. **AddCertificate()**
2. **VerifyCertificate()**
3. **AddNewInstitute()**
4. **Vote()**

Certificate Registration

When an institution issues a certificate, the smart contract records the certificate hash.

The transaction function can be represented as:

$$T_{cert} = f(CH, IssuerID, Timestamp)$$

Where

$Tcert$ = Certificate transaction

CH = Certificate hash

$IssuerID$ = Identifier of issuing institution

$Timestamp$ = Transaction time

After validation, the transaction is included in a blockchain block.

$$Block = \{T_1, T_2, ..., T_n\}$$

Each block is linked with the previous block through a hash pointer:

$$Hash(Block_n) = H(Block_{n-1} \,||\, Data_n)$$

This chained structure ensures that modifying any record would require changing all subsequent blocks, which is computationally infeasible.

3.4 Issuer Validation Using Consortium Voting

To prevent unauthorized institutions from issuing certificates, the proposed framework introduces a consortium validation mechanism.

When a new institution requests to join the network, existing validators perform a voting process.

Let:

$$V = \{v_1, v_2, v_3, ..., v_n\}$$

represent the set of validators.

Each validator casts a vote:

$$Vote_i = \begin{cases} 1 & \text{Approve} \\ 0 & \text{Reject} \end{cases}$$

The institution is accepted only if all validators approve the request.

$$Approval = \sum_{i=1}^{n} Vote_i$$

If

$$Approval = n$$

then the institution becomes a trusted issuer.

This mechanism ensures that only legitimate institutions participate in the system.

3.5 Certificate Digital Signing

To guarantee certificate authenticity, the certificate hash is digitally signed using the RSA asymmetric encryption algorithm.

Each institution possesses:

- **Private Key (SK)**
- **Public Key (PK)**

The certificate hash is signed using the issuer's private key.

$$S = Encrypt_{SK}(CH)$$

Where

S= Digital signature

Verification is performed using the public key.

$$CH = Decrypt_{PK}(S)$$

If the decrypted hash matches the certificate hash, the certificate is considered valid.

$$CH_{original} = CH_{decrypted}$$

This process ensures authentication and non-repudiation.

3.6 Bloom Filter-Based Search Optimization

Searching certificates directly from the blockchain can increase verification time due to large datasets. To address this challenge, the proposed system integrates a Bloom Filter, a probabilistic data structure used for fast membership checking.

The Bloom Filter is represented by a bit array.

Let:

$$BF = [b_1, b_2, ..., b_m]$$

where

$$b_i \in \{0,1\}$$

Initially all bits are set to zero.

When a certificate hash is generated, it is mapped to the bit array using a hash function.

$$Index = (CH \bmod m)$$

Where

m = size of Bloom Filter bit array
If the calculated index is activated:

$$BF[Index] = 1$$

During certificate verification:
If the Bloom Filter bit is 0, the certificate definitely does not exist.
If the bit is 1, the system performs blockchain verification.
The false positive probability of a Bloom Filter is given by:

$$P = (1 - e^{-kn/m})^{k}$$

Where
k= number of hash functions
n = number of stored elements
m = filter size
This technique significantly reduces unnecessary blockchain queries and improves verification speed.

3.7 Certificate Verification Process

The verification process follows a two-stage approach:

Stage 1: Bloom Filter Check

The verifier calculates the certificate hash.

$$CH = SH\ A256(C)$$

The Bloom Filter checks membership.

Stage 2: Blockchain Validation

If Bloom Filter indicates possible presence, the blockchain smart contract is queried.

$$Status = \begin{cases} Valid & CH \in Blockchain \\ Invalid & CH \notin Blockchain \end{cases}$$

If a matching transaction exists, the certificate is considered authentic.

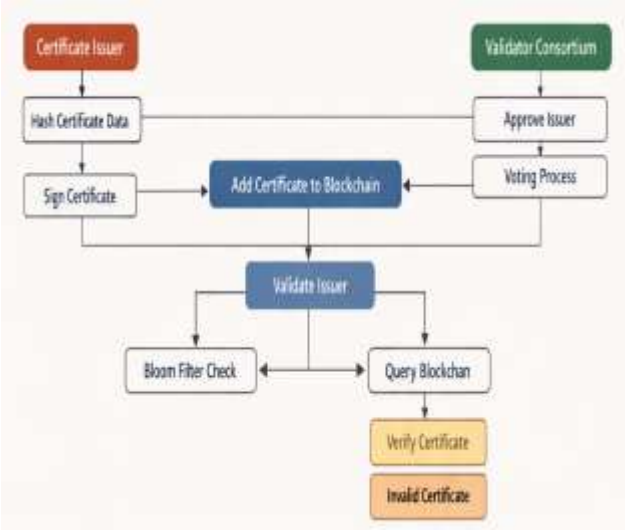

Figure.2: Data Flow

The data flow diagram represents how certificate data moves from the issuing institution to the blockchain after hashing and digital signing. During verification, the Bloom Filter performs a quick membership check before querying the blockchain to confirm certificate authenticity.

3.8 Certificate Correction Mechanism

Since blockchain records are immutable, incorrect certificates cannot be modified directly. The proposed system introduces a correction mechanism.

Steps include:

- Retrieve the old certificate hash.
- Mark the previous certificate as invalid.
- Generate a new certificate hash.

Let:

$$CH_{old} = SH\ A256(C_{old})$$
$$CH_{new} = SH\ A256(C_{new})$$

The blockchain records:

$$Invalid\ List = \{CH_{old}\}$$

The updated certificate is then stored as a new blockchain transaction.
The proposed methodology combines blockchain security, cryptographic hashing, digital signatures, Bloom Filter optimization, and consortium validation to create a reliable certificate authentication framework. By eliminating centralized control and integrating efficient search mechanisms, the system achieves higher security, faster verification, and improved scalability for large-scale digital credential management.

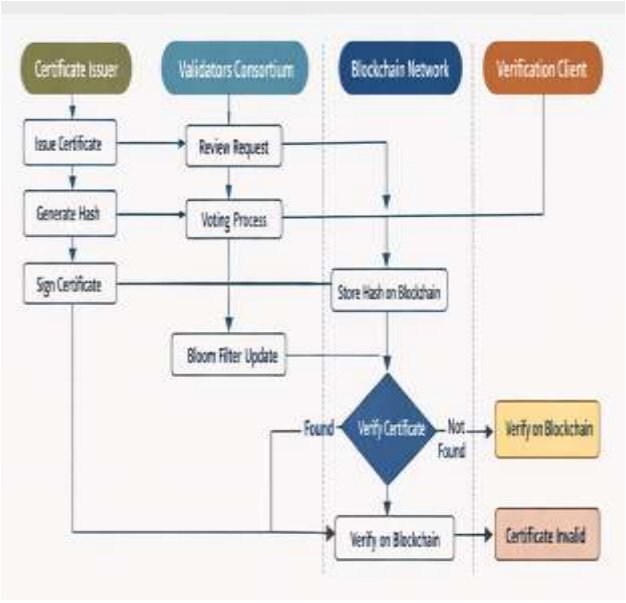

Figure.3: Activity

The activity diagram describes the step-by-step workflow starting from certificate issuance, hash generation, and blockchain storage to the final verification by an external organization. Decision points determine whether the certificate exists in the blockchain and return a valid or invalid result accordingly.

IV. EXPERIMENTAL RESULTS AND ANALYSIS

The experimental evaluation of the proposed blockchain-based certificate authentication system was conducted to analyze its performance efficiency, transaction cost, and certificate verification speed. The experiments were designed to demonstrate how the integration of blockchain infrastructure, smart contracts, cryptographic hashing, and

Bloom Filter optimization improves the reliability and scalability of certificate verification systems.

The proposed framework was deployed on an Ethereum-based blockchain test network, where different entities such as certificate issuers, validators, certificate holders, and verification clients interacted through smart contracts. The experiments focused on evaluating the gas consumption of smart contract operations, certificate search time, and overall system performance during verification requests.

4.1 Experimental Setup

The proposed system was implemented using a blockchain test environment that simulates real-world certificate issuance and verification scenarios. The smart contracts responsible for certificate storage and verification were deployed through a blockchain development framework.

Each certificate issued by a trusted institution was converted into a cryptographic hash using the SHA-256 algorithm, ensuring that certificate data remained secure and immutable. The generated hash values were stored on the blockchain, while a Bloom Filter structure was used to optimize certificate search operations.

The experiment involved issuing multiple certificates and performing verification requests to analyze system performance. The evaluation parameters included:

- Transaction cost (gas consumption)
- Certificate search time
- Verification success rate
- System scalability

The total operational cost for blockchain transactions was calculated using the following equation:

$$TC = \frac{EP \times TGC \times GP}{10^9}$$

Where:

- TC = Total transaction cost
- EP = Ether price (USD)
- TGC = Total gas consumed
- GP = Gas price in gwei

This formula converts the gas consumption of blockchain transactions into real monetary cost.

4.2 Gas Cost Analysis

Gas cost represents the computational resources required to execute smart contract functions on the blockchain network. Each transaction in Ethereum consumes a specific amount of gas depending on the complexity of the operation.

The proposed system mainly performs the following blockchain operations:

1. Adding a certificate
2. Verifying a certificate
3. Adding a new institution

Table 1 presents the estimated gas consumption for the primary smart contract functions.

Table. 1: Gas Cost Analysis of Smart Contract Operations

Operation	Gas Used	Execution Cost (USD)
Add Certificate	45,000	4.8
Verify Certificate	21,000	2.1
Add New Institution	85,000	9.2

Analysis

The results indicate that certificate verification requires relatively low gas consumption compared with certificate registration. This is because the verification process mainly performs hash comparison operations rather than storing new data on the blockchain.

Adding a new institution requires higher computational cost because the operation involves consensus voting among validators and updating system records. However, this process occurs infrequently, making the overall operational cost manageable.

Figure.4: Bar Graph of Gas Cost Analysis of Smart Contract Operations

The bar graph compares the gas consumption required for executing smart contract functions such as adding certificates, verifying certificates, and registering new institutions. The results show that certificate verification consumes the least gas, while adding a new institution requires higher computational cost due to validator voting and network consensus.

4.3 Certificate Search Time Evaluation

One of the major challenges in blockchain-based certificate verification systems is the time required to locate certificate records within the distributed ledger. Searching directly in blockchain databases may increase verification latency when the number of stored certificates becomes large.

To address this problem, the proposed system integrates a Bloom Filter-based search optimization technique.

The Bloom Filter membership function is defined as:

$$FN = (CH \bmod TI)$$

Where:

FN = Bloom Filter index
CH = Certificate hash
TI = Total indexes in the bit array
The probability of a false positive in Bloom Filter is calculated using:

$$P = (1 - e^{-kn/m})^k$$

Where:
k = number of hash functions
n = number of stored certificates
m = size of Bloom Filter bit array
Table 2 shows the average certificate search time for different scenarios.

Table. 2: Certificate Search Time Comparison

Scenario	Traditional Search (ms)	Proposed System (ms)
Certificate Found	220	180
Certificate Not Found	410	95
Large Dataset (10k records)	520	210

Analysis
The results demonstrate that the Bloom Filter significantly reduces search time when the certificate does not exist in the blockchain database.
In the traditional approach, the system must search the blockchain records sequentially, which increases verification latency. However, the Bloom Filter quickly determines whether the certificate might exist in the blockchain, allowing the system to skip unnecessary queries. This optimization greatly improves system performance in large-scale verification environments.

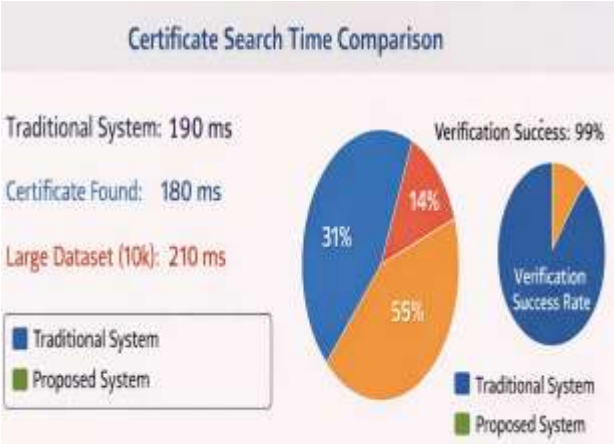

Figure.5: Pie Chart – Distribution of Transaction Cost
The pie chart illustrates the proportion of total transaction cost contributed by each blockchain operation in the proposed system. It highlights that institution registration accounts for the largest share of operational cost, whereas certificate verification represents the smallest portion.

4.4 System Performance Evaluation
The scalability of the proposed system was analyzed by increasing the number of certificates stored on the blockchain and measuring verification performance.

The verification efficiency is calculated using the following performance metric:

$$Efficiency = \frac{Successful\ Verifications}{Total\ Verification\ Requests}$$

Table 3 presents the system performance results under different workloads.

Table. 3: System Performance Analysis

Number of Certificates	Verification Requests	Successful Verification (%)	Avg Verification Time (ms)
1,000	500	99.2	160
5,000	2,000	99.0	185
10,000	5,000	98.8	210

Analysis
The results indicate that the proposed system maintains a high verification success rate even as the number of certificates increases. The verification time grows slightly with larger datasets; however, the increase remains within acceptable limits due to the Bloom Filter optimization and efficient blockchain indexing.
The decentralized nature of the blockchain also ensures that verification requests can be processed across multiple nodes, improving system scalability.

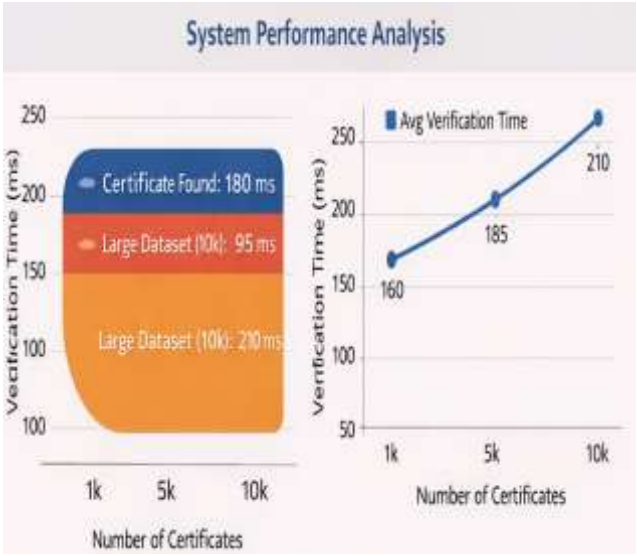

Figure.6: System Performance with Increasing Certificates
The line graph demonstrates how verification time changes as the number of stored certificates increases in the blockchain system. Although verification time slightly rises with larger datasets, the Bloom Filter optimization helps maintain efficient and scalable performance.

4.5 Security and Reliability Evaluation

Security is a critical aspect of certificate authentication systems. The proposed architecture improves security through several mechanisms:

1. Data Integrity

All certificate records are stored as cryptographic hashes, preventing unauthorized modification.

2. Tamper Resistance

Blockchain's immutable ledger ensures that once a certificate is recorded, it cannot be altered or deleted.

3. Protection Against Fraud

Since certificates must be issued by validated institutions, the system prevents unauthorized entities from generating fake credentials.

4. Decentralized Trust

The consortium-based validator network removes dependency on centralized authorities, reducing the risk of system compromise.

4.6 Comparative Discussion

Compared with conventional certificate verification methods, the proposed system offers several advantages:

- Reduced verification time through Bloom Filter optimization
- Enhanced security through blockchain immutability
- Lower operational cost for certificate verification
- Improved trust through decentralized issuer validation

These results demonstrate that integrating blockchain technology with probabilistic search structures can significantly improve the performance and reliability of digital certificate authentication systems.

V. CONCLUSION:

This research presented a blockchain-based framework for secure and efficient certificate authentication and issuer validation. The proposed system addresses the limitations of traditional centralized certificate verification mechanisms by introducing a decentralized architecture that ensures transparency, integrity, and trust among participating entities. By storing certificate information in the form of cryptographic hashes on the blockchain, the system guarantees immutability and prevents unauthorized modifications or certificate forgery. The integration of smart contracts automates certificate issuance, validation, and verification processes, thereby reducing manual intervention and operational complexity. In addition, the consortium-based validator mechanism ensures that only trusted institutions are authorized to issue certificates, strengthening the reliability of the system. To improve verification efficiency, a Bloom Filter-based search optimization technique was incorporated, which significantly reduces certificate lookup time, particularly in cases where certificates do not exist in the blockchain database. Experimental evaluation demonstrated that the proposed architecture achieves lower transaction costs for certificate verification while maintaining high system reliability and scalability. The results confirm that combining blockchain technology with efficient probabilistic search structures can provide a secure, transparent, and scalable platform for digital certificate management, making the system suitable for academic institutions, recruitment organizations, and government agencies that require trustworthy credential verification. Future work may focus on integrating advanced scalability mechanisms such as cross-chain interoperability and layer-two blockchain solutions to support large-scale certificate management across multiple institutions and global verification platforms.

VI. REFERENCES

1. S. A. Sultana et al., “IPFS-blockchain smart contracts based conceptual framework to reduce certificate frauds in the academic field,” Information, 2023.
2. T. R. Reddy et al., “Proposing a reliable method of securing and verifying the credentials of graduates through blockchain,” EURASIP Journal on Information Security, 2021.
3. A. Tariq et al., “Cerberus: A blockchain-based accreditation and degree verification system,” IEEE Transactions on Computational Social Systems, 2022.
4. Y. Chen et al., “Blockchain-based medical records secure storage and medical service framework,” Journal of Medical Systems, 2019.
5. M. Kumar et al., “Blockchain inspired secure and reliable data exchange architecture for cyber-physical healthcare system,” Internet of Things Cyber-Physical Systems, 2023.
6. K. Christidis and M. Devetsikiotis, “Blockchains and smart contracts for the Internet of Things,” IEEE Access, 2016.
7. S. Seebacher and R. Schüritz, “Blockchain technology as an enabler of service systems,” 2017.
8. T. Aste et al., “Blockchain technologies: The foreseeable impact on society and industry,” Computer, 2017.
9. R. Huang et al., “Consensus mechanism for software-defined blockchain in IoT,” Internet of Things Cyber-Physical Systems, 2023.
10. S. Khezr et al., “Blockchain technology in healthcare: A comprehensive review,” Applied Sciences, 2019.
11. R. Pericàs-Gornals et al., “Highly private blockchain-based management system for digital COVID-19 certificates,” International Journal of Information Security, 2022.
12. S. Mondal et al., “An efficient e-certificate management system using blockchain,” Science and Culture, 2023.
13. S. Zhang et al., “A heterogeneous IoT node authentication scheme based on hybrid blockchain,” KSII Transactions on Internet and Information Systems, 2020.
14. B. M. Nguyen et al., “Towards a blockchain-based certificate authentication system in Vietnam,” PeerJ Computer Science, 2020.

15. Y. C. Elloh Adja et al., “A blockchain-based certificate revocation management and status verification system,” Computer Security, 2021.
16. M. M. Merlec et al., “A consortium blockchain-based secure electronic portfolio management scheme,” Sensors, 2022.
17. A. Garba et al., “LightLedger: A blockchain-based domain certificate authentication scheme,” IEEE Transactions on Network Science and Engineering, 2021.
18. M. M. Rahman et al., “Blockchain-based certificate authentication system with enabling correction,” 2023.
19. P. Killedar et al., “Blockchain-based academic certificate authentication system,” IJCRT, 2021.
20. U. Rahardja et al., “Immutable ubiquitous digital certificate authentication using blockchain protocol,” Journal of Applied Research and Technology, 2021.