IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 24 December 2024, accepted 29 January 2025, date of publication 4 February 2025, date of current version 12 February 2025.

Digital Object Identifier 10.1109/ACCESS.2025.3539180

RESEARCH ARTICLE

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

ROJALINA PRIYADARSHINI[1], (Member, IEEE), RHISHAV PANDEY[1], K. C. ANKIT[1], DEEPESH BHANDARI[1], BIRENDRA KHADKA[1], RABINDRA KUMAR BARIK[2], (Member, IEEE), AND MANOB JYOTI SAIKIA[3,4], (Senior Member, IEEE)

[1]Department of Computer Science and Engineering, C. V. Raman Global University, Bhubaneswar 752054, India
[2]School of Computer Applications, KIIT Deemed to be University, Bhubaneswar 751024, India
[3]Electrical and Computer Engineering Department, The University of Memphis, Memphis, TN 38152, USA
[4]Biomedical Sensors and Systems Lab, The University of Memphis, Memphis, TN 38152, USA

Corresponding author: Manob Jyoti Saikia (msaikia@memphis.edu)

This research and the APC were funded by the Biomedical Sensors & Systems Lab, The University of Memphis, Memphis, TN, USA.

ABSTRACT Verifying the legitimacy of original documents such as educational degree certificates is crucial. If these are found to be fraudulent, it can cause significant disruptions in the hiring process, resulting in substantial productivity losses. The researchers suggested several proposals to preserve these certificates. However, the challenge is still to have an integrated, tamper-proof and low-cost solution where the certificate issuer and the certificate itself are validated in a single platform. This paper proposes an integrated solution that uses a decentralized blockchain-based certificate verification and issuer validation system. In addition to this, it will protect the certificates from being tampered with. To search faster, hash function mapping has been employed. The proposed solution is experimentally validated by creating a blockchain network using Ethereum where each peer node represents an entity of a certificate verification system such as a validator, certificate issuer, certificate holder and the end-user of the client. The performance of the designed solution is measured by the execution and transaction cost in terms of gas consumption. A comparative analysis has been performed on similar types of tasks reported in the existing work performed on the same platform. It has been observed that the cost incurred for adding a certificate is minimal for the proposed approach. Furthermore, the searching time for the certificates is minimized by using a hash-based searching methodology. The results show that the search time has drastically gone down when certificates are not available.

INDEX TERMS Blockchain, certificate verification, authentication, Ethereum, search optimization.

I. INTRODUCTION

The management of certificates, particularly ensuring their integrity and tamper-resistance, is a critical issue in today's digital world. Traditional public-key certificates stored in distributed databases offer some level of security, but they are not immune to vulnerabilities like central points of failure, making them less ideal for ensuring the authenticity of certificates over time.

Targeting cloud data, the highest result of all verticals analyzed was that the majority of educational organizations experienced phishing attacks (60%) and account compromise (33%) in 2020 [1]. Due to such threats, academic certificates issued by educational institutions are susceptible to forgery.

Hiring a candidate with false qualifications can cost a company an average of $15,000 [2]. Moreover, there may be considerable social harm: apart from a compromised sense

The associate editor coordinating the review of this manuscript and approving it for publication was Mahdi Zareei.

of ethics, a fake degree holder will likely not possess the requisite expertise in his field (achieved through rigorous training and evaluation), thereby posing a real danger in certain domains.

The traditional defense against fake credentials is stringent verification procedures [3]. Manual verification, though still utilized, is an outdated approach that lags in today's fast-paced digital landscape, increasing the risk of errors. These interruptions, exacerbated by time-consuming traditional methods, expose significant security vulnerabilities. Reliance on centralized authorities in conventional methods creates a single point of failure vulnerable to cyber attacks. Even temporary downtime or data loss in such systems can disrupt academic and hiring processes, leading to significant operational inefficiencies. Additionally, this flaw opens the door to certificate fabrication, undermining the foundational trust these systems aim to uphold. Traditional distributed databases provide a certain degree of decentralization but still rely on centralized control for key operations such as access management, data backup, and updates. This centralized control creates vulnerabilities, including the potential for single points of failure and susceptibility to tampering. For instance, if the central authority managing the database is compromised, unauthorized modifications or data breaches can occur, undermining trust in the system. Additionally, traditional systems lack inherent transparency, as stakeholders cannot independently verify the authenticity of records without relying on the central authority.

Blockchain, as another internet generation, has the potential to solve these issues [4]. Blockchain has become the prominent technology to ensure the security and privacy of user data and is used in several applications like healthcare, transportation, agriculture, smart home, supply chain, etc [5]. Blockchain technology has attracted considerable attention from academics over the past few years [6].

Blockchain technology's distributed ledger and tamper-proof features make it an ideal solution for certificate validation and authentication. In transactions, people introduce ''smart contracts'' through programs and algorithms, apply blockchain technology to ensure the integrity and reliability of transactions [7]. Once stored on the blockchain, the credibility of certificates becomes unquestionable, eliminating the possibility of unauthorized modifications [8]. Furthermore, blockchain eradicates the single point of failure inherent in traditional methods. Unlike traditional methods, blockchain enables peer-to-peer transfer of digital assets without any intermediaries [9]. Its decentralized network ensures that a compromised node cannot compromise the integrity of the validation infrastructure as a whole.

In this paper, we present a blockchain-based approach that addresses critical issues in certificate verification. The proposed solution ensures that certificate records are tamper-proof by using blockchain technology, which makes it impossible to alter or forge the information once it is recorded. Additionally, the system incorporates smart contracts to enable secure and transparent updates to certificates, allowing for necessary corrections without compromising data integrity. By operating on a decentralized network, the approach eliminates the reliance on a single central authority, thus reducing the risk of errors and increasing the reliability of the authentication process. Moreover, the use of a Bloom Filter optimizes the verification process, making it faster and more cost-effective compared to other methods.This proposed solution offers decentralized certificate authentication using smart contracts and makes use of blockchain technology to guarantee the integrity and immutability of the certificate records [10].

A hash function is used for mapping certificate elements to a bit array, which improves the speed of the verification process by reducing unnecessary computations, especially for false negatives, and optimizing search time. This optimization is particularly critical in high-demand scenarios, such as large-scale university admissions, where thousands of certificate verifications may need to be processed within tight deadlines. In addition, a thorough system security check is performed using a static analysis framework tool for vulnerability identification to discover and neutralize such threats. The study focuses on applying, evaluating, and contrasting design techniques with other approaches to validate the proposed methodology, showing its uniqueness and efficiency. The key contributions outlined in this work are as follows:

- **Novel Blockchain Integration:** We propose a novel blockchain-based architecture that ensures decentralized, tamper-proof, and transparent validation of certificates and issuers, therefore increasing the reliability of authentication systems.
- **Hash-Based Optimization:** By employing a hash function mapping to a Bloom Filter, the system significantly reduces the certificate search time, particularly minimizing false negatives and unnecessary computations.
- **Enhanced Security Mechanisms:** The proposed architecture uses Ethereum's hybrid permission mode to guarantee security and integrity while incorporating strong defenses against well-known threats like 51% and Sybil attacks.
- **Cost-Effective Implementation:** Experimental results demonstrate a lower transaction cost for certificate addition compared to existing systems, making the proposed solution more accessible and scalable.
- **Scalability and Flexibility:** The framework facilitates easy integration with trusted institutions, ensuring the seamless addition of new participants through an automated and transparent voting mechanism.

The remainder of this paper is organized as follows. Section II reviews related work, highlighting the limitations of existing solutions. Section III details our proposed architecture and the specific role of blockchain and smart contracts in our system. Section IV discusses the experimental evaluation of our approach, focusing on performance and security metrics. Finally, Section V concludes the paper.

II. LITERATURE REVIEW

Pericàs-Gornals et al. [11] proposed a privacy-preserving approach for managing digital COVID-19 certificates on a blockchain. It addresses the need for privacy and security in health data management, allowing users control over their data while regulating certificate generation and validation entities. The protocol combines proxy re-encryption services with blockchain, offering easy verification and preventing forgery. However, this approach is tailored specifically for health data management and does not scale well to other types of certificates. Furthermore, the reliance on a private network limits its accessibility and raises questions about the credibility of information outside the specific network.

TABLE 1. Literature review.

S.No	Author	Relevant Concepts	Limitations
1	Pericàs-Gornals et al. [11]	Proxy Re-Encryption	Network validation required
2	Mondal et al. [12]	Verification without intermediaries	Random node addition
3	Zhang et al. [13]	Efficiency with consortium blockchain	Unmanaged private blockchain communication
4	Nguyen et al. [14]	Blockchain analysis in decentralized applications	Affects institutional control
5	Adja et al. [15]	Bloom Filter on public blockchain	Not suitable for large volumes
6	Merlec et al. [16]	Consortium blockchain for secure management	Limited flexibility in access control
7	Garba et al. [17]	Zero-knowledge proofs and Bloom Filter	Browser plugin required and expensive verification process
8	Rahman et al. [18]	Hybrid blockchain for certificate issuance	Undefined validation mechanisms
9	Kiledar et al. [19]	User-friendly interface for certificate issuance	High operational cost, no validation
10	Rahardja et al. [20]	Hashed certificates by authorized validators	Slow PDF certificate verification
11	Lamkoti et al. [21]	Automated certificate generation and validation	Open validator registration
12	Turkanović et al. [22]	Integration using REST API	Centralized database presence
13	Ghani et al. [23]	Hyperledger Fabric with e-certificate framework	Local database vulnerability

Table 1 is not a comparative analysis, but rather a summary of findings from comparable studies that are relevant to our research. The 'Relevant Concepts' column emphasizes key concepts, methodologies, or frameworks from each work that influenced or contributed to our approach. The 'Limitations' column emphasizes features of these studies that were not relevant or aligned with our objectives, emphasising areas where our research seeks to improve. Similarly, Mondal et al. [12] present a blockchain-based system for efficient and secure e-certificate management. Certificates are stored in IPFS with cryptographic hashes, enabling verification without intermediaries. Elliptic Curve Cryptography (ECC) provides secure encryption and decryption. However, the system doesn't highlight the certificate searching process, which is a critical aspect of our focus. Moreover, the way institutions communicate via private blockchain is not addressed. Zhang et al. [13] introduce a system using consortium blockchain for component management. This system also doesn't address our main concerns, as it focuses on component management and doesn't offer a robust solution for certificate management.

The study of Nguyen et al. [14] explored the use of blockchain in decentralized applications, business process integration, and data mapping. They highlighted design considerations and offered insights into blockchain-based authentication systems. While Adja et al. [15] addressed limitations of Public Key Infrastructure (PKI) by proposing a decentralized revocation system using blockchain, Merlec et al. [16] introduced a consortium blockchain-based scheme for secure e-portfolio management. A Bloom Filter on a public blockchain efficiently stores and revokes certificate information. The immutable ledger ensures data integrity and eliminates reliance on trusted third parties.

The work by Garba et al. [17] implemented a system for certificate authentication that strengthens privacy with zero-knowledge proofs and uses a Bloom Filter for efficient Certificate Authority (CA) list management. Despite of increased performance in the proposed approach of Garba et al. [17], the selection of the validator is random. Also, it requires a browser extension plug-in to get a certificate and query the trusted certificate authority list. Rahman et al. [18] proposed a novel approach for blockchain-based certificate authentication with correction mechanisms. A two-chain architecture separated certificate data from corrections, enabling universities to issue corrected certificates. This system is deployed and granted access to the network to a single University. They could not define the presence of validation authority to verify certificates. Killedar et al. [19] developed a user-friendly Dapp interface for both administrators and students, streamlining certificate issuance and verification processes.

Likewise, Rahardja et al. [20] analyzed the application of blockchain for a tamper-proof and globally accessible digital certificate authentication system. Their framework leverages blockchain to create an immutable record of certificates, enhancing trust and accessibility. Similarly, Lamkoti et al. [21] proposed a blockchain-based framework for securing transcript generation and certificate validation. This approach offered faster transcript generation and addressed challenges in verifying academic credential authenticity. The system allowed anyone to register themselves as validators creating a lack of reliability inside the system.

Turkanović et al. [22] introduced EduCTX, a blockchain-based infrastructure for monitoring credits in higher education. This system provides a secure and tamper-proof record of student achievement, promoting global recognition of academic credentials.

Ghani et al. [23] developed a permissioned blockchain network for managing and distributing student credentials. This system utilizes Hyperledger Fabric to offer secure and tamper-proof records, with smart contracts controlling

data access. This study develops a permissioned blockchain network for managing and distributing student credentials. This system utilizes Hyperledger Fabric to offer secure and tamper-proof records, with smart contracts controlling data access.

Given these limitations, there is a clear need for a decentralized system to manage certificates reliably and securely across different domains. Our proposed solution addresses this need by using a blockchain-based framework, which enhances both efficiency and security.

III. PROPOSED ARCHITECTURE

This paper presents a blockchain-based system designed to verify the validity of institutions issuing certificates and to confirm the authenticity of those certificates. The system is divided into two primary components: the front end, where users interact, and the back end, where the blockchain framework operates, as illustrated in Figure 1.

In the front end, institutions act as certificate issuers. These institutions request the validation of certificates they issue by interacting with the blockchain network. The front end collects user inputs and sends the requests to the back end, where the blockchain and Bloom Filter components are located. The blockchain network consists of a consortium of institutions responsible for validating the certificate issuers. A smart contract deployed on the public blockchain records the votes on the issuer's validation and stores certificate data. After validating the certificate issuer, the system pushes the certificate information to the blockchain, where it is securely stored. The Bloom Filter is then updated to optimize search times during the certificate verification process.

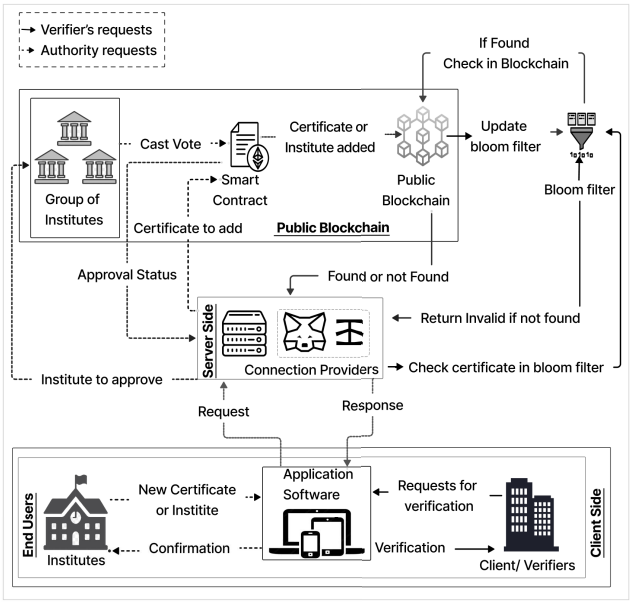

FIGURE 1. Architecture of certificate verification system.

Verifiers, who need to check the authenticity of a certificate, interact with the back-end through connection providers. These providers retrieve the requested details from the blockchain. After a successful transaction, verifiers receive confirmation of the certificate's validity. The architecture involves several key roles and entities, which are explained in detail below:

- **Validator:** The blockchain is secured by a group of trusted institutions. These institutions are responsible for creating, distributing, and verifying certificates within the network. Only institutions within this trusted group can perform transactions on the blockchain, making any certificate issued by a member automatically considered valid.

  Institutions that belong to this group are referred to as validators. Validators designated as "trusted institutions" who have the sole authority of issuing certificates and cast votes for new institutions that wish to join the trusted group which maintain the system's general authenticity. The purpose of this strict classification is to guarantee that only reliable organizations are permitted to take part within network operations. Figure 2 illustrates how validators manage the certificate life cycle within the system. For a new institution to become a trusted issuer, it must receive approval from all existing members of the group.

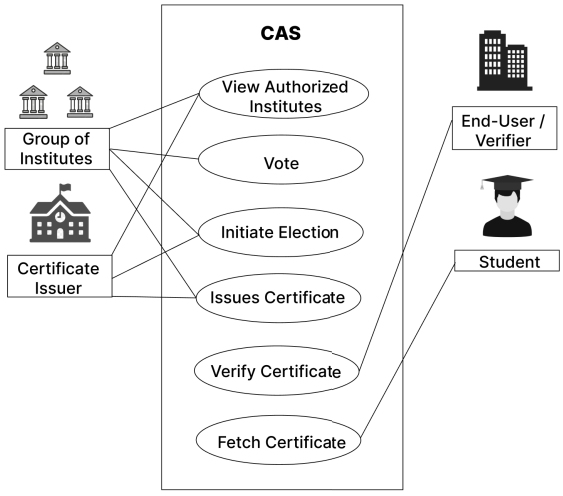

FIGURE 2. Different features of certificate authentication system (CAS).

- **Certificate Issuer:** Within the blockchain network, certain institutions are responsible for issuing certificates. However, not all institutions have the same level of trust. Any institution can technically issue a certificate, but only those designated as "trusted" by the validator group can issue certificates that are automatically recognized as valid.This mechanism ensures the authenticity and reliability of certificates issued within the blockchain.
- **Certificate Holder:** The certificate holder is the person or entity for whom the certificate is issued. These individuals or organizations own the certificates and can use them for various purposes, such as academic

achievements or professional qualifications. The system allows certificate holders to share their certificates when required, ensuring that they are easily verifiable by external parties.

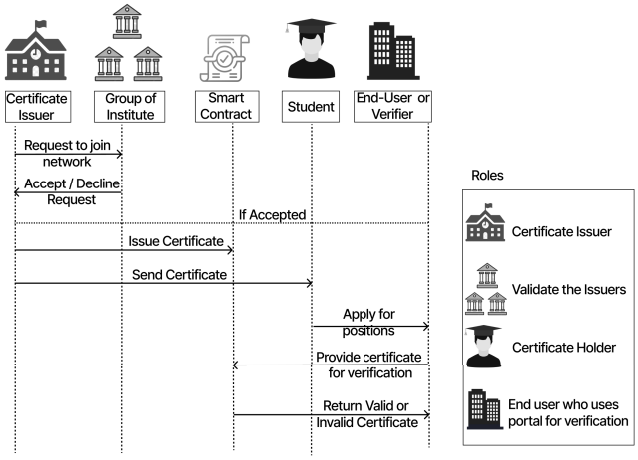

FIGURE 3. Certificate validation process by the verifier organization.

- **Client/Verifier:** Clients, or verifiers, are individuals or organizations that need to verify the validity of a certificate. Verifiers rely on the blockchain to confirm the authenticity of a certificate. They can view blockchain transactions, but unlike validators, they cannot participate in the validation process. Verifiers are end-users of the system, accessing it through a user-friendly interface. Their role is crucial in ensuring that certificates presented to them are legitimate and trustworthy.

Each of these roles plays an important part in the overall success of the certificate validation process, as shown in Figure 3. The system allows any verifying organization to access a designated portal, where they can check the validity of an issued certificate quickly and securely.

A. DEPLOYMENT OF SMART CONTRACTS

The smart contract is used to automate key processes such as adding trusted institutions, deploying certificates, and verifying certificate status on the blockchain. These contracts ensure a secure and decentralized validation mechanism, eliminating manual intervention and reducing processing time. The smart contracts streamline the operations within the blockchain network, enhancing transparency and reliability.

Our system's architecture integrates a smart contract that is deployed on the Sepolia testnet using Remix IDE. It is configured with MetaMask for seamless blockchain interaction. The deployment uses Infura to connect to a Sepolia node, and assigns the contract a unique testnet address. The front-end application, developed in JavaScript, utilizes Web3.js to enable secure and efficient communication with the blockchain. Institutions add certificates by hashing data in the front-end and invoking the smart contract using Web3.js, which also updates on Bloom Filter for optimized search. During verification, the front-end first checks the Bloom Filter before querying the blockchain for final validation.

The smart contract deployed on the Sepolia testnet facilitates decentralized certificate and institution management through key functions: addCertificate, verifyCertificate, NewInstitute, and Vote. The addCertificate function stores certificate hashes on-chain and updates a Bloom Filter for efficient search, while verifyCertificate uses the Bloom Filter for validation before confirming authenticity on the blockchain. The addNewInstitute function allows trusted authorities to propose institutions, and Vote enables validators to cast votes, ensuring that only approved institutions can participate.

Table 2 summarizes the key smart contract functions and their roles in the system.

TABLE 2. Key smart contract functions.

Function	Purpose and Outcome
AddCertificate()	Adds a certificate to the blockchain; ensures uniqueness by storing only new hashes.
VerifyCertificate()	Verifies certificate status by matching its hash on the blockchain.
NewInstitute()	Initiates voting for institution inclusion into the trusted network.
Vote()	Casts votes to approve or reject new institutions; finalizes inclusion process.

Likewise, gas fees are charged when a smart contract is deployed; this is a common occurrence in blockchain systems. Every transaction carried out by the smart contract contains a gas fee, which represents the processing power used in completing the transaction.

B. VALIDATION OF A NEW INSTITUTE

The addition of a new institute implies that if it is trusted, it gains the authority to issue valid certificates. For a new institute to deploy a valid certificate, it must first be recognized as a trusted institute through the voting process. Once an institute is trusted, it becomes part of the existing network, where all trusted institutes collectively participate in certificate issuance and validation. Any new institute must still undergo the same voting process before being added to the trusted list, as illustrated in Figure 4.

- Request to join as a trusted institute: The first step in joining a trusted institute is for any institute to submit a request to join.
- Request Initialization: After receiving this request, existing institutes begin the configuration procedure. This involves all already existing institutes participating in an election.
- Voting for new institute: All present institutes in the network vote for new institutes. If any one member mistrusts this new institute or disapproves its request, then the new institute cannot join as an authorized institute.

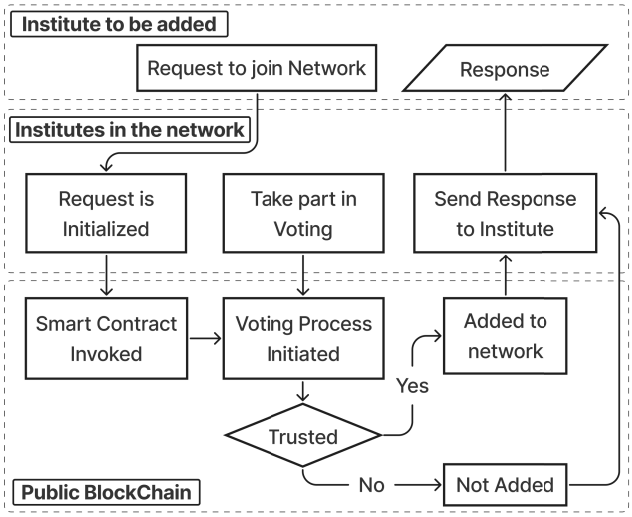

FIGURE 4. Inclusion of a new institute in the network.

- Decision Making: The Institute gets included in the network if it is trusted by all existing institutes that are trusted inside the network. Likewise, the institute is not included in the network even if it is not trusted by at least one existing trusted institute inside the network. Thus, new institutes must gather a hundred percent votes from trusted institutes inside the network.
- Chaincode Invoked: Once the new institute is trusted inside the network, it gets access to copies of all transactions inside the network. Now, this new institute can read, write, and access the information. This also illustrates that the certificate issued by this specific institute will be considered valid.

C. ISSUING OF CERTIFICATE BY TRUSTED INSTITUTES

If the institute is already trusted, all the certificates issued by that particular institute are considered to be valid by default. This procedure is initiated by a certificate being issued by a trusted institute as depicted in Figure 5.

- Hash generation: Within the blockchain, each certificate issued by a trusted institution is processed through a smart contract, which generates a unique hash for the certificate. This hash acts as a digital fingerprint, ensuring that any alteration to the certificate would result in a different hash, thereby signaling tampering. Additionally, our system introduces an additional layer of hashing to optimize the search process within the network.
- Transaction Execution and Validation: The smart contract uses the generated hash to execute and validate transactions. Validation ensures that only authorized institutions can issue certificates, enhancing the system's reliability. These processes adhere to standard blockchain mechanisms, ensuring that transactions meet consensus rules.
- Transaction Broadcasting: After validation, the transaction is included in a block and broadcasted to the blockchain network. This ensures that the certificate is securely stored on the public blockchain and cannot be altered or removed.

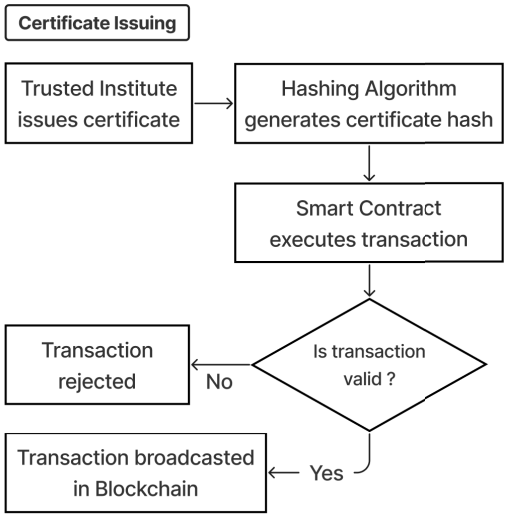

FIGURE 5. Certificate issue and broadcasting through network.

D. SIGNING OF CERTIFICATE

Encryption and decryption of the hash of the certificate happens as demonstrated in Figure 6. In the proposed system, the RSA (Rivest-Shamir-Adleman) algorithm is used to digitally sign the hash of the certificate, ensuring its authenticity and integrity. The trusted institutes use their private keys to sign the hash, which uniquely identifies the certificate. This signed hash is stored immutably on the blockchain.

The signing process ensures that any entity receiving the certificate can verify its validity by retrieving the signed hash from the blockchain and decrypting it using the public key of the issuing institute. If the decrypted hash matches the hash of the presented certificate, the certificate is deemed valid and untampered. This approach is based on RSA's asymmetric cryptographic nature, where the private key is used for signing and the public key is used for verification [24].

E. MECHANISM FOR SEARCH TIME OPTIMIZATION

To minimize the certificate search time in the blockchain network a hashed mapping technique is used as depicted in Figure 7. A basic probabilistic data structure based on bit-array works by hashing entries to quickly determine whether or not they belong in a collection. Implementation of the hashing algorithm enables the hashing of the certificate and its subsequent indexing into this finite array.

The inclusion of a Bloom Filter in our system is driven by the need for fast and efficient searches, particularly in situations where certificates must be verified in real time, such as during job applications or academic admissions. The

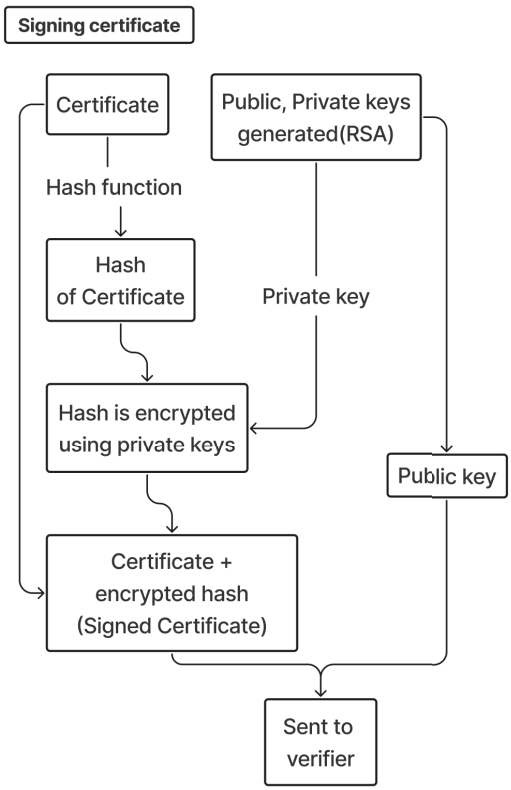

FIGURE 6. Certificate signing process.

Bloom Filter is a probabilistic data structure that allows for quick checks to determine whether a certificate exists in the blockchain. While there is a small chance of false positives, this trade-off is acceptable given the significant reduction in search times, as shown by our experimental results.

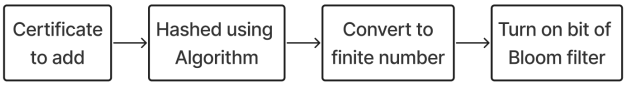

FIGURE 7. Process for search optimization.

The Bloom Filter, represented as a bit array, maps this hashed information. Since it operates with an 'on' or 'off' mechanism, one piece of information only occupies 1 bit. In this system bit array of size 1 MB is used, thus, the Total number of indexes(TI) is 8,388,608.

By default, all the index in the bit array is represented by an 'off' state of '0'. To map the certificate hash to a bit array, the hash is converted into a finite number as shown in Equation 1:

$$FN = (CH) \mod TI \tag{1}$$

where:

FN : Finite number

CH : Certificate Hash

TI : Total number of indexes in the bit array

After obtaining a finite number, that particular index in the array is turned 'on' and this state of the Filter is mapped with certificate hash. An 'on' state ('1'), indicates that the certificate is present on the public blockchain. This array now helps in the searching process when verifiers are willing to verify certificate status.

F. CORRECTION OF DEFECTIVE CERTIFICATES

Blockchain being an immutable ledger, editing, and deleting of information in the chain is impossible. There may be some cases where certificate holder might find any credentials of their certificate wrong such as name, marks, address, subjects, etc., and many more. In such cases, they request their respective certificate issuer for correction of their already issued certificates. After the institute receives the request, correction happens as illustrated in Figure 8.

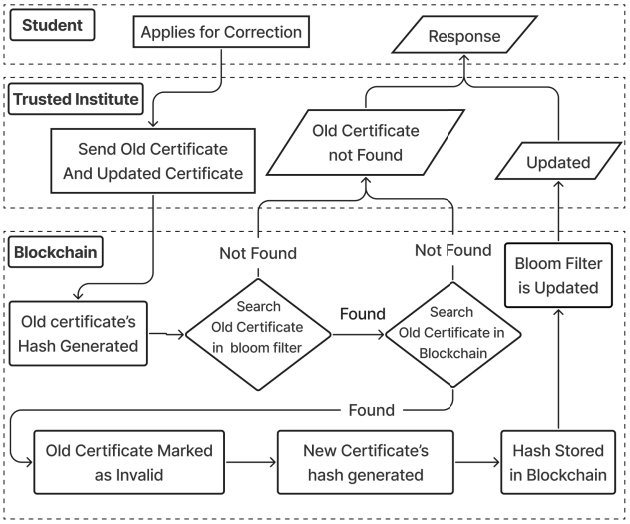

FIGURE 8. Process for correction of certificates.

- Student Application: A student discovers an error in their certificate and applies for a correction.
- Trusted Institute's Role: The institute responsible for issuing certificates receives applications from the certificate holder. It checks whether the certificate is previously validated or not in the Bloom Filter. If the Bloom Filter indicates the certificate is new (not found), the validation process terminates, and a response is provided.
  However, if the Bloom Filter suggests the certificate might have been issued before (found), the certificate issuer retrieves both old and updated certificates for further verification and push into the blockchain.
- Blockchain Validation: To ensure the certificate's validity, the system verifies its presence within the blockchain. The presence of the old certificate is checked in the blockchain by calculating the hash of the old certificate by using SHA-256.
  When the hash of the old certificate matches with any existing hash in the chain, the certificate is previously

valid, thus, correction can be done. If the certificate cannot be located on the blockchain, it signifies that the certificate has not undergone the validation process beforehand. Consequently, the process will halt and respond.

Records in blockchain are unchangeable. A list is created in the blockchain for marking defective certificates generated. Since the old certificate is found, the hash of the old certificate is kept in this list inside the blockchain. All certificates in this list are marked as invalid and cannot be used.

Now, the hash of the new certificate is generated using a similar hashing mechanism as described in section III-C. This new hash is then stored in the blockchain and all processes are repeated as mentioned in section III-C. Thus, wrongly issued or defective certificates are corrected in the system and provided to the certificate holder as mentioned in section III-D.

G. VERIFICATION OF CERTIFICATE STATUS

Within the scope of a public blockchain, the verification process takes place. For the certificate verification to be visible and accessible to all parties, this integration of public blockchain is essential, as shown in Figure 9. Requests of such kind can be easily fulfilled via the assigned front-end interface, making use universal accessibility of public blockchain. This promotes a simple, open verification procedure that builds a common trust model.

Verifying clients or entities can check whether the certificate is authentic or not through a designated portal through which certificate details on the blockchain network can be viewed. On viewing certificate details of any specific certificate, the certificate issued from a trusted and validated institute from within the network is considered valid and other certificates are considered to be invalid.

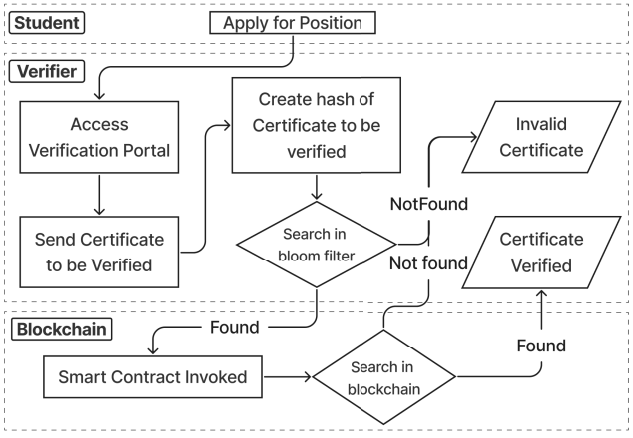

FIGURE 9. Process diagram for verification of certificate.

When credentials are found to match, the certificate receives validation status, confirming its integrity and authenticity. Else the certificate submitted to the verification portal is considered incorrect or fake.

- Submission: A certificate holder uses a certificate for various purposes in various organizations.
- Request to Blockchain: The verifying organization sends a request to the blockchain network to check the certificate's authenticity.
- Verification: The hash of the certificate submitted through the user interface is checked against the Bloom Filter. If the filter is of state 'off' (i.e. 0), the certificate is considered to be invalid and the verification process terminates. To maintain validation integrity within the blockchain ecosystem in such cases, the verifier can ask the certificate holder to start the process of re-validation with the relevant issuing institute.

  If the Bloom Filter indicates 'on' (i.e. 1), the smart contract which contains logic for checking certificates is called that further searches the certificate inside the blockchain.
- Result: The blockchain returns a confirmation of the certificate's validity or an alert if discrepancies are found.
- Organization Decision: Based on the blockchain's verification, the organization proceeds with the application process.

Even if a verifier attempts to check the validity of a defective certificate, the certificate will be considered invalid, as that has been identified as invalid in section III-F.

IV. RESULT & DISCUSSION

This section discusses the cost and security aspects of the proposed solution deployed on the Ethereum blockchain. Firstly, costs associated with running the contracts on the network are analyzed. Secondly, the presented solution is compared to existing blockchain-based solutions to highlight its strengths and potential advantages. Finally, a thorough security analysis is conducted through Slither of the smart contracts to ensure their robustness and mitigate any potential vulnerabilities.

A. COST ANALYSIS

This section analyzes the gas costs associated with the Ethereum smart contract code and function calls. On the Ethereum blockchain, executing a transaction incurs a gas fee. The Remix IDE is a valuable and user-friendly tool for estimating gas costs. There are two primary categories of gas costs: execution cost and transaction cost. Execution cost refers to the computational expense of running various smart contract functions. Transaction cost includes the cost of any data transmitted to the blockchain network. The cost is calculated as shown in equation 2.

$$TC = \frac{EP * TGC * GP}{1000000000} \tag{2}$$

where:

TC : Total Cost of Operation in USD
EP : Ether Price in USD
TGC : Total Gas Cost
GP : Gas price in gwei
1 Ether : 1000000000 gwei

The table 3 details the gas costs associated with deploying smart contracts and their functions. Similarly, Figure 12 & Table 4 shows the cost comparison of the proposed system with existing solutions. For the proposed system

TABLE 3. Cost analysis.

Operation	Execution Gas	Transaction Gas	Cost in USD
Deploying	1712381	1697740	156.21
Adding Certificate	50088	49699	4.57
Initiate Election	98450	97480	8.97
Voting	139237	128640	12.27

adding a certificate incurs a lower cost compared to existing solutions, while adding an institution has a slightly higher cost. However, adding an institution is a one-time expense. Further work is needed to make this process more affordable and convenient. The gas fees are converted to USD for easy comparison with existing solutions. The average gas price is 22 Gwei and the price of ether is USD 2082.24, retrieved on November 24, 2023, from etherscan.io, which was used for the conversion. It is important to note that gas prices fluctuate over time, and the values used here may not be accurate in the future. However, they are intended to illustrate that the cost of executing these functions is generally quite low.

Gas fees on the Ethereum blockchain are subject to network congestion, demand fluctuations, and market conditions. During peak activity periods, such as NFT minting events or high transaction volumes, gas prices can spike significantly, potentially increasing the cost of certificate issuance and verification. This variability poses a challenge for institutions, particularly those issuing certificates in bulk, as operational costs could escalate unpredictably.

TABLE 4. Cost comparison.

Operations	Proposed CAS	R. Pericàs-Gornals et al. [11]	Elva Leka et al. [25]
Adding Certificate	4.57	14.32	8.24
Adding Institutes	8.97	19.06	4.35

B. CERTIFICATE SEARCH TIME

This subsection describes the time a smart contract takes to search for a certificate hash stored within it. Two scenarios are considered for certificate verification: true (certificate exists) and false (certificate does not exist).

In the true case, the certificate hash is found in the blockchain, while in the false case, the certificate does not exist. The Bloom Filter significantly reduces search time in the false case, as the system quickly identifies that the certificate is not present, reducing unnecessary blockchain queries. However, in the true case, the search time with the

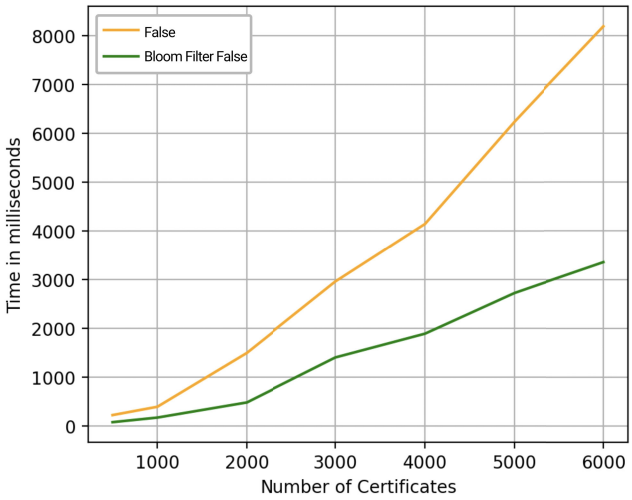

FIGURE 10. Certificate search time for false case.

Bloom Filter is slightly longer because the Bloom Filter adds step before confirming the certificate's existence in the blockchain. This trade-off is acceptable because the Bloom Filter drastically improves performance in the false case, as illustrated in Figure 10. The results indicate a noticeable performance improvement in scenarios where the certificate does not exist, which is critical for large-scale systems with numerous verification requests.

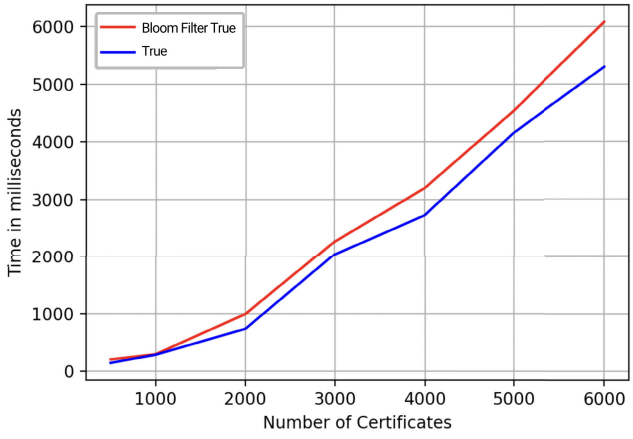

FIGURE 11. Certificate search time for true case.

C. COMPARISON WITH EXISTING SOLUTIONS

Table 5 compares the proposed solution to existing blockchain-based solutions. Parameters like the blockchain

network, permission mode, validating authority, cryptocurrency, voting mechanism, use of centralized storage, and Bloom Filter are considered for comparison with existing approaches. Existing systems for certificate authentication

TABLE 5. Comparison with existing solutions.

	Proposed Solution	[20]	[23]	[11]	[25]
Blockchain Network	Ethereum	Ethereum	ARK	Ethereum	Hyperledger Fabrics
Permission Mode	Hybrid	Public	Public	Private	Private
Validating Authority	Group of institution	None	None	WHO	None
Crypto Currency	Ether	Ether	Ark	Ether	-
Voting Mechanism	Yes	No	No	No	No
Centralized Storage Mechanism	No	Yes	Yes	No	Yes
Bloom Filter	Yes	No	No	No	No

utilize blockchains like ARK and Hyperledger Fabric. However, the proposed system leverages the Ethereum blockchain network with a hybrid permission mode. Using a public blockchain network with hybrid permission ensures both transparency and integrity during certificate authentication. A consortium of institutes acts as validating authorities, granting trustworthiness as only recognized institutions can issue certificates. The proposed system eliminates the use of a centralized storage database throughout the process. This approach avoids a single point of failure and prevents counterfeiting. Furthermore, the proposed Certificate Authentication System (CAS) incorporates a Bloom Filter to optimize certificate verification time, which is absent in other approaches.

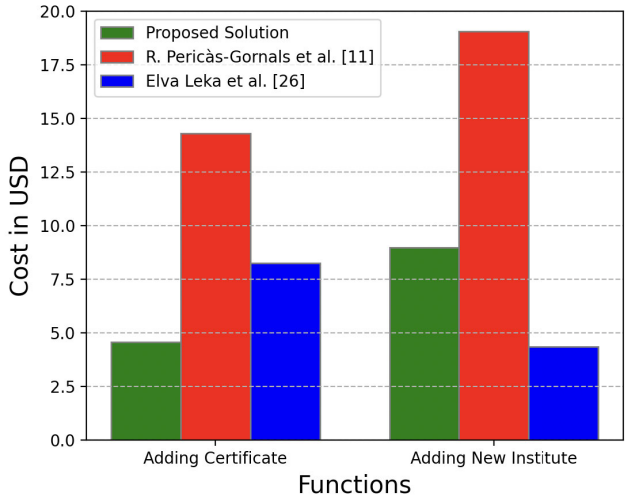

FIGURE 12. Cost comparison with existing solutions.

D. COMPARASION OF PROPOSED SYSTEM IN TERMS OF NFT USING IPFS IMPLEMENTATION

In this paper, we propose a blockchain-based solution for certificate verification without relying on NFTs (Non-Fungible Tokens) using IPFS (InterPlanetary File System). While NFTs are useful for cases where ownership of a digital asset needs to be established, they are not necessary in our system because university certificates consist of information that needs verification, not ownership. For instance, the utilization of NFTs in medical services allows medical data, such as X-rays, test reports, and prescriptions, to be represented as digital assets stored on distributed ledger technology (DLT), ensuring each asset is uniquely identifiable, tamper-proof, and securely managed by patients [26]. Instead, we hash the certificate data using SHA-256 and store the resulting hash on the blockchain. Since SHA-256 produces a fixed-size output of 256 bits (32 bytes), the size of the transaction remains small and efficient. When combined with typical blockchain metadata which includes addresses, transaction ID, gas fees, timestamps, and signatures, the total transaction size is 182 bytes in our proposed system. In cases where the entire certificate files need to be stored like medical report [27], IPFS could play a pivotal role by allowing large files to be stored off-chain and referenced on the blockchain but since we only store the hash and verification is done through hash, the implementation of IPFS is not necessary in this case. A work by Sharma et al. [28] uses the interplanetary file system to store the metadata of e-commerce products to avoid storing large amounts of data on the blockchain. Our approach ensures that the certificate verification process is secure, lightweight, and cost-effective by minimizing the size of the transaction while maintaining data integrity.

E. SECURITY ANALYSIS OF PROPOSED ARCHITECTURE

1) 51% ATTACK

Blockchain technology offers many advantages for secure certificate authentication. A major concern is the potential for a 51% attack, where a malicious entity gains control of more than half of the computing power on the network. This dominance allows them to manipulate transaction history, potentially enabling them to issue fraudulent certificates or revoke valid ones. This proposed system is based on Ethereum blockchain which is a Proof-of-Stake (PoS) that increases the cost of such attacks. Additionally, a group of trusted institutes participate through a voting mechanism, adding another layer of validation. In this system, an assumption is made that, a p proportion of the network is controlled by independent full nodes. This distributed ownership structure makes it computationally infeasible for an attacker to acquire enough control to achieve a 51% attack and manipulate the system. Even if an attacker gained control of a significant portion of the network (i.e. $p \leq \frac{1}{2}$), they would still need to join trusted institutes that adhere to the group validation process, significantly increasing the attack complexity.

2) SYBIL ATTACK

In a Sybil attack, a malicious actor creates numerous fake identities to manipulate the system. To combat Sybil attacks, the proposed system restricts each institute to a single account. This restricts the creation of fake identities for manipulating the system. Furthermore, institutes seeking validator status undergo background checks by existing, trusted validators, followed by a voting process for inclusion. This multi-layered approach, combining account limitations with a trusted selection process, significantly reduces the risk of Sybil attacks and fosters a secure environment for certificate authentication.

3) IMMUTABILITY

Immutability is an inherent characteristic of blockchain technology that ensures data, once recorded, cannot be altered or deleted. Once a certificate is issued and validated, it becomes an immutable part of the blockchain ledger. This creates a permanent record that eliminates the risk of unauthorized modifications. As a result, the authenticity and validity of a certificate can be guaranteed throughout its existence. Additionally, the tamper-proof nature of blockchain makes it impossible to compromise the integrity of certificates. This immutability fosters trust in the certificate verification process.

4) DATA PRIVACY

Blockchain technology offers a secure and transparent approach to certificate authentication, but its inherent transparency can raise concerns about data privacy. Our proposed system addresses this by employing a privacy-preserving method that stores only cryptographic hashes of certificates on the public Blockchain. A cryptographic hash function transforms the certificate data into a unique, irreversible string of characters, ensuring that the original content cannot be reconstructed from the hashed value, thereby protecting sensitive information. Once hashed, trusted institutions digitally sign the certificate along with the public key of the certificate holder. This process ensures the certificate's authenticity while preserving privacy. The signed certificate is then delivered to the certificate holder, who can decrypt it using their private key. This decrypted certificate can be shared with various entities as needed, ensuring control over the data while maintaining security and privacy. The public Blockchain retains its transparency by allowing verification of the hash, but the one-way nature of the hash function ensures that the original certificate content remains private and secure from unauthorized access.

F. STATIC SECURITY ANALYSIS OF SMART CONTRACT

Static analysis is a debugging technique that examines source code without executing it. It is particularly crucial for smart contracts due to their immutable nature. Once deployed on the blockchain, the code cannot be modified, meaning any vulnerabilities or bugs become permanent and could lead to significant losses. In this study, we performed static analysis on the smart contract responsible for key functionalities, including certificate issuance, validation, and voting (AddCertificate, VerifyCertificate, and Vote functions). The analysis was conducted using the Slither framework, a Python-based tool designed for Ethereum smart contracts. Slither works by converting Solidity smart contracts into an intermediate representation called SlithIR [29]. This framework identifies vulnerabilities, optimizes code, and assists with code reviews. The results of the static analysis presented in Figure 13, demonstrate that the analyzed smart contract is secure. No medium- or high-level vulnerabilities were detected, with only one low-severity issue identified. The scope of this analysis was limited to the core smart contract and did not include auxiliary scripts or off-chain components. This focused analysis ensures a strong foundation for the blockchain implementation.

```
Number of low issues: 1
Number of medium issues: 0
Number of high issues: 0

+---------------------+-------------+------+-----------+--------------+----------+
| Name                | # functions | ERCS | ERC20 info | Complex code | Features |
+---------------------+-------------+------+-----------+--------------+----------+
| CertificateRegistry |          14 |      |           |           No |          |
+---------------------+-------------+------+-----------+--------------+----------+
INFO:Slither:updatedsol.sol analyzed (1 contracts)
```

FIGURE 13. Security analysis using slither.

V. CONCLUSION

This paper describes a secure and reliable system for verifying the authenticity of certificates. The system is designed to be tamper-proof, decentralized, and completely transparent. To achieve data privacy, the system makes use of hash functions. To ensure the legitimacy of issued certificates, a voting mechanism participated by existing institutions authorizes new certificate issuers. The system utilizes a Bloom Filter to efficiently search for certificates that enable fast verification.

The approach presented in this paper significantly reduced verification time, particularly for certificates that are ultimately found to be invalid. Additionally, the proposed system is resilient to 51% attacks and Sybil attacks. The paper presents a static analysis of the implemented smart contract using the open-source Slither framework. Cost and system approach comparison with existing methods highlights the efficiency and effectiveness of the proposed system. The comparison shows that the cost of adding a new certificate is comparatively less whereas the cost of adding a new institute is comparable with existing approaches.

VI. FUTURE WORKS

While the current implementation optimizes certificate search time using hashed mapping techniques and a Bloom Filter, for system to accommodate a significantly larger number of certificates and users, more advanced blockchain mechanisms can be implemented. To enable smooth communication across various platforms, future research might

focus on creating standardized APIs or middleware solutions. These developments would guarantee improved flexibility in the system and consistent validation of information. Although the current implementation achieves lower transaction costs than existing systems, further optimizations are necessary to ensure economic feasibility for institutions with limited resources.

REFERENCES

[1] S. A. Sultana, C. Rupa, R. P. Malleswari, and T. R. Gadekallu, "IPFS-blockchain smart contracts based conceptual framework to reduce certificate frauds in the academic field," *Information*, vol. 14, no. 8, p. 446, Aug. 2023.
[2] T. Rama Reddy, P. V. G. D. Prasad Reddy, R. Srinivas, C. V. Raghavendran, R. V. S. Lalitha, and B. Annapurna, "Proposing a reliable method of securing and verifying the credentials of graduates through blockchain," *EURASIP J. Inf. Secur.*, vol. 2021, no. 1, pp. 1–9, Dec. 2021.
[3] A. Tariq, H. B. Haq, and S. T. Ali, "Cerberus: A blockchain-based accreditation and degree verification system," *IEEE Trans. Computat. Social Syst.*, vol. 10, no. 4, pp. 1503–1514, Aug. 2022.
[4] Y. Chen, S. Ding, Z. Xu, H. Zheng, and S. Yang, "Blockchain-based medical records secure storage and medical service framework," *J. Med. Syst.*, vol. 43, no. 1, pp. 1–9, Jan. 2019.
[5] M. Kumar, H. Raj, N. Chaurasia, and S. S. Gill, "Blockchain inspired secure and reliable data exchange architecture for cyber-physical healthcare system 4.0," *Internet Things Cyber-Phys. Syst.*, vol. 3, pp. 309–322, Jan. 2023.
[6] S. Khezr, M. Moniruzzaman, A. Yassine, and R. Benlamri, "Blockchain technology in healthcare: A comprehensive review and directions for future research," *Appl. Sci.*, vol. 9, no. 9, p. 1736, Apr. 2019.
[7] R. Huang, X. Yang, and P. Ajay, "Consensus mechanism for software-defined blockchain in Internet of Things," *Internet Things Cyber-Phys. Syst.*, vol. 3, pp. 52–60, Jan. 2023.
[8] S. Seebacher and R. Schüritz, "Blockchain technology as an enabler of service systems: A structured literature review," in *Proc. Int. Conf. Exploring Services Sci.*, Jan. 2017, pp. 12–23.
[9] T. Aste, P. Tasca, and T. Di Matteo, "Blockchain technologies: The foreseeable impact on society and industry," *Computer*, vol. 50, no. 9, pp. 18–28, 2017.
[10] K. Christidis and M. Devetsikiotis, "Blockchains and smart contracts for the Internet of Things," *IEEE Access*, vol. 4, pp. 2292–2303, 2016.
[11] R. Pericàs-Gornals, M. Mut-Puigserver, and M. M. Payeras-Capellà, "Highly private blockchain-based management system for digital COVID-19 certificates," *Int. J. Inf. Secur.*, vol. 21, no. 5, pp. 1069–1090, Oct. 2022.
[12] S. Mondal, A. Panja, and S. Karforma, "An efficient e-certificate management system in e-learning using blockchain," *Sci. Culture*, vol. 89, nos. 3–4, pp. 1–5, Apr. 2023.
[13] S. Zhang, Y. Cao, Z. Ning, F. Xue, D. Cao, and Y. Yang, "A heterogeneous IoT node authentication scheme based on hybrid blockchain and trust value," *KSII Trans. Internet Inf. Syst. (TIIS)*, vol. 14, no. 9, pp. 3615–3638, 2020.
[14] B. M. Nguyen, T.-C. Dao, and B.-L. Do, "Towards a blockchain-based certificate authentication system in Vietnam," *PeerJ Comput. Sci.*, vol. 6, p. e266, Mar. 2020.
[15] Y. C. Elloh Adja, B. Hammi, A. Serhrouchni, and S. Zeadally, "A blockchain-based certificate revocation management and status verification system," *Comput. Secur.*, vol. 104, May 2021, Art. no. 102209.
[16] M. M. Merlec, M. M. Islam, Y. K. Lee, and H. P. In, "A consortium blockchain-based secure and trusted electronic portfolio management scheme," *Sensors*, vol. 22, no. 3, p. 1271, Feb. 2022.
[17] A. Garba, Z. Chen, Z. Guan, and G. Srivastava, "LightLedger: A novel blockchain-based domain certificate authentication and validation scheme," *IEEE Trans. Netw. Sci. Eng.*, vol. 8, no. 2, pp. 1698–1710, Apr. 2021.
[18] M. M. Rahman, M. T. K. Tonmoy, S. R. Shihab, and R. Farhana, "Blockchain-based certificate authentication system with enabling correction," 2023, *arXiv:2302.03877*.
[19] P. Killedar, L. M. Pranav, N. S. Bhat, R. Math, and S. J. Shetty, "Blockchain based academic certificate authentication system," *Int. J. Creative Res. Thoughts (IJCRT)*, vol. 9, no. 7, pp. 477–484, Jul. 2021. [Online]. Available: http://www.ijcrt.org/papers/IJCRT2107283.pdf
[20] U. Rahardja, A. N. Hidayanto, P. O. H. Putra, and M. Hardini, "Immutable ubiquitous digital certificate authentication using blockchain protocol," *J. Appl. Res. Technol.*, vol. 19, no. 4, pp. 308–321, Aug. 2021.
[21] D. Maji, R. S. Lamkoti, H. Shetty, and B. Gondhalekar, "Certificate verification using blockchain and generation of transcript," *Int. J. Eng. Res. Technol.*, vol. 10, no. 3, pp. 1–6, Apr. 2021.
[22] M. Turkanović, M. Hölbl, K. Košič, M. Heričko, and A. Kamišalić, "EduCTX: A blockchain-based higher education credit platform," *IEEE Access*, vol. 6, pp. 5112–5127, 2018.
[23] R. F. Ghani, A. A. Salman, A. B. Khudhair, and L. Aljobouri, "Blockchain-based Student certificate management and system sharing using hyperledger fabric platform," *Periodicals Eng. Natural Sci. (PEN)*, vol. 10, no. 2, pp. 207–218, Apr. 2022.
[24] X. Zhou and X. Tang, "Research and implementation of RSA algorithm for encryption and decryption," in *Proc. 6th Int. Forum Strategic Technol.*, vol. 2, Aug. 2011, pp. 1118–1121.
[25] E. Leka and B. Selimi, "Development and evaluation of blockchain based secure application for verification and validation of academic certificates," *Ann. Emerg. Technol. Comput.*, vol. 5, no. 2, pp. 22–36, Apr. 2021.
[26] S. Rai, B. K. Chaurasia, R. Gupta, and S. Verma, "Blockchain-based NFT for healthcare system," in *Proc. IEEE 12th Int. Conf. Commun. Syst. Netw. Technol. (CSNT)*, Apr. 2023, pp. 700–704.
[27] B. K. Chaurasia, "Blockchain enabled MediVault for healthcare system," *Multimedia Tools Appl.*, vol. 2024, pp. 1–21, Jun. 2024.
[28] A. K. Sharma, B. K. Chaurasia, and V. Singh, "Blockchain-based feedback system using NFT in e-commerce," *Iran J. Comput. Sci.*, vol. 7, no. 3, pp. 579–587, Sep. 2024.
[29] J. Feist, G. Grieco, and A. Groce, "Slither: A static analysis framework for smart contracts," in *Proc. IEEE/ACM 2nd Int. Workshop Emerg. Trends Softw. Eng. Blockchain (WETSEB)*, May 2019, pp. 8–15.

ROJALINA PRIYADARSHINI (Member, IEEE) received the master's degree (Hons.) in information technology from F. M. University, Balasore, Odisha, India, in 2006, the M.Tech. degree in computer science and engineering from SOA University, Bhubaneswar, India, in 2010, and the Ph.D. degree in computer science and engineering from KIIT Deemed University, Bhubaneswar, India, in 2020.

She has published over 70 technical papers featured in esteemed journals and conference proceedings. Among them, more than 30 are in SCI-indexed journals and over 60 are Scopus-indexed articles. With over 16 years of teaching and 14 years of research experience, she is currently an Associate Professor with the Department of Computer Science and Engineering, C. V. Raman Global University, Odisha. Her research focuses on cloud/fog computing, cybersecurity, and applied machine learning. Additionally, she holds recognition as an Amazon Web Service (AWS) certified, accredited cloud educator and a Wipro-certified Java faculty. She serves as a reviewer for numerous esteemed journals.

RHISHAV PANDEY was born in Kathmandu, Nepal. He received the B.Tech. degree in computer science of engineering from C. V. Raman Global University, in 2024.

He was with Cognitive Sciences Laboratories, Indian Institute of Technology, where he was involved in interdisciplinary research that combined elements of computer science with linguistics. His current research interests include blockchain technology and its applications, along with exploring how emerging technologies can be integrated to solve complex real-world problems.

K. C. ANKIT was born in Butwal, Nepal. He received the B.Tech. degree in software engineering from C. V. Raman Global University, in 2024.

He has gained significant experience through independent research, which resulted in the publication of the article Blockchain-Based Donation Management in Disaster Response. He has presented several papers at blockchain-related conferences and has contributed to the academic community by reviewing journal articles. In addition to his technical expertise, he worked on a research project to find and present solutions for community schools in his city, where he demonstrated his ability to manage interdisciplinary projects, conduct surveys, and analyze data. His current research interests include blockchain technology, cryptocurrency, and consensus mechanisms.

DEEPESH BHANDARI received the B.Tech. degree in computer science and engineering from C. V. Raman Global University, in 2024. He is currently working on several projects related to blockchain, data analytics, machine learning, and software development. He has a passion for exploring new technologies and methodologies to solve complex problems and enhance computational efficiency. During his academic career, he has worked on various projects, including the development of blockchain applications, predictive models, data visualization tools, and software applications. He has also participated in various hackathons and coding competitions, achieving recognition for his innovative solutions, and technical skills. His research interests include blockchain, data analytics, machine learning, artificial intelligence, and software development.

BIRENDRA KHADKA received the B.Tech. degree in computer science and engineering from C. V. Raman Global University, Bhubaneshwar, Odisha, India, in 2024. His research interest includes minimizing certificate verification time in blockchain technology.

RABINDRA KUMAR BARIK (Member, IEEE) received the M.Tech. and Ph.D. degrees from the Motilal Nehru National Institute of Technology Allahabad, Prayagraj, India, in 2009 and 2014, respectively. He is currently an Associate Professor with the School of Computer Applications, KIIT Deemed to be University, Bhubaneswar, India. He was selected for MHRD scholarship during his both M.Tech. and Ph.D. He has qualified for GATE-2007 in information technology conducted by IIT-Kanpur. He is doing collaborative research with The University of Texas at Dallas and The University of Rhode Island in the field of fog computing. He has published in more than 30 international journals, such as Springer, Elsevier, and IGI Global. He has also published more than 50 conference papers in various top-level conferences, such as Global-SIP, CHASE, TENCON, and INDICON. He has more than 25 book chapters on his credit. Prior to this, he edited one book on *Cloud Computing for Geospatial Big Data Analytics: Intelligent Edge, Fog and Mist Computing* (Springer Nature) in the series of studies in big data. He is reviewing in many journals, such as Springer, Elsevier, IEEE, and IGI Global. His research interests include geospatial data science, geospatial big data infrastructure, geospatial databases, geospatial cloud computing, fog computing, and IPR. He has served as a TPC and PC members for many conferences. He is a member of IAENG. He is ranked among the World's Top 2% Scientists as per the recent study conducted by researchers of the ICSR Laboratory, Elsevier B. V. & Stanford University, USA, in 2022. He has received the Best Paper Awards at FICTA-2020, ICSCC-2017, and ICECE-2017 conferences.

MANOB JYOTI SAIKIA (Senior Member, IEEE) received the B.E. degree in electronics and communication engineering from Visvesvaraya Technological University, Belgaum, India, in 2009, the M.Tech. degree in bioelectronics from Tezpur University, Tezpur, Assam, India, in 2013, and the Ph.D. degree in electrical engineering from The University of Rhode Island, Kingston, RI, USA, in 2019.

He was an Assistant Professor with the Electrical Engineering Department, University of North Florida. He was a Research Associate with the School of Engineering, Tufts University, from September 2019 to August 2022. He was also a Senior Research Associate with the Department of Engineering, Boston College, from May 2022 to August 2022. From January 2016 to July 2019, he was a Research Assistant in a project funded by the National Science Foundation, USA. From 2012 to 2015, he was awarded a Senior Research Fellowship from the Ministry of Science and Technology, India, working at the Indian Institute of Science, Bengaluru, India. He is currently the Director of the Biomedical Sensors and Systems Laboratory and an Assistant Professor with the Electrical and Computer Engineering Department, The University of Memphis. His research interests include biomedical instrumentation, sensors, neuroimaging (fNIRS and EEG), signal processing, machine learning, and the Internet of Things.