iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 14 **Issue:** IV **Month of publication:** April 2026

DOI: https://doi.org/10.22214/ijraset.2026.81495

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 14 Issue IV Apr 2026- Available at www.ijraset.com

Transparent and Scalable Decentralized Blockchain Model for Certificate Authentication Using Search Optimization

Tamminana Dinesh[1], Mattukoyya Amulya[2] (Faculty), Addanki Jahnavi[3], Ganta Pratyusha[4], Badigunchala Ganesh[5]
Department of Cyber Security and Engineering, Acharya Nagarjuna University, Andhra Pradesh, India - 522510

Abstract: ***In the digital age, verification of academic credentials has emerged as a serious problem with the growing challenge of document forgery and dependence on centralized system. Conventional methods are slow, susceptible to mistakes, and at risk of being attacked. In this paper, we present a scalable and secure blockchain-based certificate authentication system that provides a tamper-proof and transparent validation for both certificate issuers and the issued certificates. The system uses Ethereum smart contracts and SHA-256 hashing to guarantee immutability and integrity of the data. A consensus-driven voting procedure is utilized to authenticate the trusted institutions, which prevents having a single point of trust. In addition, to improve performance, a Bloom Filter-based search optimization method is employed, resulting in a dramatic reduction on the time of certificate verification, especially for large scale environment. The proposed framework is designed with strong security and privacy guarantees to withstand attacks, e.g., Sybil attacks and 51% attacks, while maintaining user's data privacy by only depositing cryptographic hashes on the blockchain. The simulation results illustrate lower transaction costs and higher verification efficiency than other existing solutions. The technique offers a secure, decentralized, and cost-effective method to authenticate certificates in both academic and professional fields.***

Keywords: ***Blockchain, Certificate Authentication, Ethereum, Smart Contracts, SHA-256, Bloom Filter, Decentralized Verification, Data Integrity, Tamper-Proof System, Security Optimization***

I. INTRODUCTION

Authenticity and the integrity of educational certificates have become vital issues in the eyes of academia, employers and regulatory bodies in the internet era. However, due to the booming of digital documents and online hiring process, the possibility of certificate forging and credential fraud was dramatically increased. The existing certificate verification methods are often based on centralized databases and manual verification processes, these verifications are time-consuming, inefficient and error-prone. Also, centralized systems can be compromised by cyberattacks, data tampering, and single points of failure, shaking the confidence in the verification mechanism.

A recent study revealed that a majority of companies suffering from fake credentials find their business affected financially and operationally. Current methods of verification have intermediaries, making the processes longer and costly, and are not transparent. These constraints motivated for development of a secured, transparent and decentralized solution for document authentication.

The nature of blockchains has made the related technology a potential solution to challenges. Employing distributed ledger, blockchains make once recorded data immutable to provide a high level of data trustworthiness and integrity. Smart contracts also improve the automation potential by defining rules for certificate issuance, validation and verification automatically without human intervention.

In this paper, we present a decentralized certificate authentication system based on blockchain that authenticates not only a certificate issuer but also a certificate in a decentral manner.

The system utilizes Ethereum smart contract and SHA-256 hashing to store certificate contents as hashes in the block chain, providing immutability and data privacy. And the consensus-based voting protocol is proposed to select and authorize trust-worthy institutions to further improve the system and remove the single point of trust.

To cope with scalability and performance issues, we introduce a search optimization based on Bloom Filter into the system. This can greatly expedite the time for verifying certificates especially when a large number of requests are to be served at the same time and in large scale. The proposed system includes security features to prevent common blockchain attacks such as Sybil and 51% attacks.

The major contributions of the work are as follows:

- A decentralized and fair certificate authentication scheme using blockchain.
- A two-layer verification process for both certificates issuers and certificates.
- Bloom Filter-based Certificate Search Optimization.
- Development of a secure voting procedure for the validation of trusted institutions.
- An efficient and scalable scheme with enhanced verification performance.

II. LITERATURE REVIEW

The issue of certificate verification has attracted much attention in the recent few years as a result of rampant document tampering and inadequacy of conventional verification system. A number of researchers have suggested the use of blockchain-based solutions for improving the security, transparency, and performance of certificate validation methods.

Pericàs-Gornals et al. introduced a privacy-preserving blockchain architecture for digital certificate management, with a special emphasis on COVID-19 health certificates. They embed proxy re-encryption techniques to protect the confidentiality of data and enable privacy-preserving verification. Nevertheless, it is domain specific and cannot be extended to general academic certificate validation.

Mondal et al., proposed a blockchain-enable e-certificate system where they handled the issue. Though secure storage and verification of the system is achieved, an efficient search scheme is lacking, which is indispensable for large-scale construction.

Garba et al. proposed a blockchain based certificate authentication scheme using bloom Filters to enhance search efficiency. Although their approach improves the performance, the validator selection is by random, this could lead to loss of trust and security in the network.

Rahman et al. introduced a bitcoin-inspired certificate framework with correction using a dual-chain model. Thus, institutions can correct erroneous certificates while preserving historical records. But the system does not have a strong validation authority system, and therefore its trust model is limited.

Turkanović et al. proposed Edu CTX - a decentralized global higher education credit platform based on blockchain. It ensures an immutable record of students' achievement and makes it globally accessible. Although the system is controlled on credit rather than certificate, it has benefits.

Ghani et al. built a permissioned blockchain system with Hyperledger Fabric to manage student credentials. Their solution facilitates secure data sharing and access control through smart contracts. But the need to trust a permissioned network reduces transparency and decentralization.

There are some existing systems that take advantage of technologies like IPFS and NFTs to save certificate data. In contrast, these solutions for managing large files and ownership introduce more complexity and cost to the system. In addition, they are not always needed when certificate verification can be done via hash-based verification.

From above works, we can conclude that although blockchain based certificate authentication possesses a very promising future, current approaches suffer from several drawbacks such as no efficient search scheme is provided, no robust validator selection scheme is constructed, no tool method is introduced to help reduce high working cost nor is the system approached towards scalability.

To address these issues, we propose a decentralized blockchain-based certificate authentication model, which is based on a consensus-driven validators framework as well as Bloom Filter-based search optimization. This ensures verification is secure, efficient, and scalable yet transparent and trusted by all network participants.

III. AIMS OF THE STUDY

This work is intended to design and build a novel system, based on blockchain, that is secure, decentralized and efficient in terms of certificate authentication and revocation. The proposed system seeks to address the inherent shortcomings of traditional verification techniques by introducing transparency, integrity, and scalability in verification.

The study has the following specific objectives:

1) To design a certificate authentication framework based on blockchain which meets the requirements of preventing certificate data from being tampered with and stored in a non-volatile manner.

2) We're deploying a two-pronged validation process: One to establish that certificates are authentic, and the other to validate the issuing institution.

3) To applying cryptographic hashing (SHA-256) to secure certificate data and to protect privacy by storing on the blockchain only the hash values.
4) To design and implement Ethereum smart contracts for certificate issuance, validation and verification are presented.
5) To add a bloom Filter based search optimization technique to minimize certificate verification time and increase the performance of the system.
6) To create a consensus-based voting scheme to select and empower trusted organizations within the network.
7) To improve the defence of the system against common blockchain attacks including Sybil and 51% attacks.
8) To support scalability and cost effectiveness for wide spread usage in educational and professional fields.
9) To accomplish these goals helps in establishing the reliability and transparency of the certificate authentication procedure, which intensifies the level of trust followed by institutions, students, and employers.

IV. RESEARCH METHODOLOGY

To address these issues, this paper proposes a new system based on blockchain technology that guarantees a secure, decentralized, and efficient process for certificate authentication. The approach combines cryptography, smart contracts and search optimization techniques in order to obtain trustful certificates and certificate authorities.

A. *System Design*: An overview of the design of the proposed system is given below.

The system is based on a decentralized design with four key types of entities: validators, certificate issuers, certificate holders, and verifiers. Validators are reputable organizations that maintain the blockchain ledger and validate other organizations through a consensus-based voting process. Certificate issuers create and upload certificates, whilst certificate holders hold them and share them when needed. Verifiers (such as employers or other institutions) authenticate the certificates via the system.

B. *Certificate Generation and Hashing*

When a certificate is signed, the SHA-256 cryptographic hash function is applied to its data to create a single digital fingerprint. This hash guarantees the integrity of the data, because a change in the certificate will lead to a different hash value. Rather than holding the real certificate, a hash on the certificate is stored on the blockchain, to keep privacy and to ease the storage need.

C. *Smart Contract Implementation*

Ethereum smart contracts are used to facilitate certificate issuance and verification and institutional validation. Major functions include adding certificates, verifying certificate authenticity, registering new institutions, and voting processes. These smart contracts remove the need for manual intervention, and deliver transparency, correctness, and trust to the system.

D. *Validation by Consensus-Based Institution*

In order to keep the network trusted, a consensus-based voting system is employed. Any new institution that requests to be part of the network will have to be accepted by all the rest of the trusted validators. This ensures that only confirmed and reputable organizations can issue certificates which makes the system stronger as a whole.

E. *Search Optimization Using Bloom Filter*

This is managed using a bloom-filter based search optimization method included within the protocol. The Bloom Filter is a probabilistic data structure which allows to quickly establish if a given certificate exists as a member or not of the set. A certificate hash is turned into a bit array when it is added. The verification system checks the Bloom Filter first in the verification process, and if it's negative, invalidates the certificate right away, without querying blockchains unnecessarily. If it is, the blockchain is then queried to make sure. This reduces the time to verify significantly, especially for high scale systems.

F. *Certificate Verification*

The validation process is initiated when a verifier enters certificate information in the system interface. A certificate hash is computed and queried against the Bloom Filter. If filter returns yes, hash is checked on the blockchain via smart contract. A match means the certificate is genuine, while a non-match means a fake certificate is detected and/or an invalid certificate.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 14 Issue IV Apr 2026- Available at www.ijraset.com

G. Security Assurance

The above system has many layers of security that any potential attacker or hacker would have to breach. In addition, the immutability of blockchain discourages data tampering and cryptographic hashing guarantees the integrity and privacy of data. Consensus-based validation mitigates Sybil attacks by decreasing the number of unauthorized votes. Besides, the distributed structure of the blockchain reduces the chances of 51% attacks, and promotes security of the system.

H. Evaluations of the Performance

The performance of the system is evaluated in terms of the transaction cost and the search time of the certificate. Gas costs are calculated for smart contract functions and search

V. PROPOSED SYSTEM

In this proposed system, we introduce a decentralized and secure certificate authentication system based on the blockchain technique. The system is intended to overcome the constraints of the standard verification system by providing accountability, immutability, and the efficient verification of certificate providers as well as the certificates they provide.

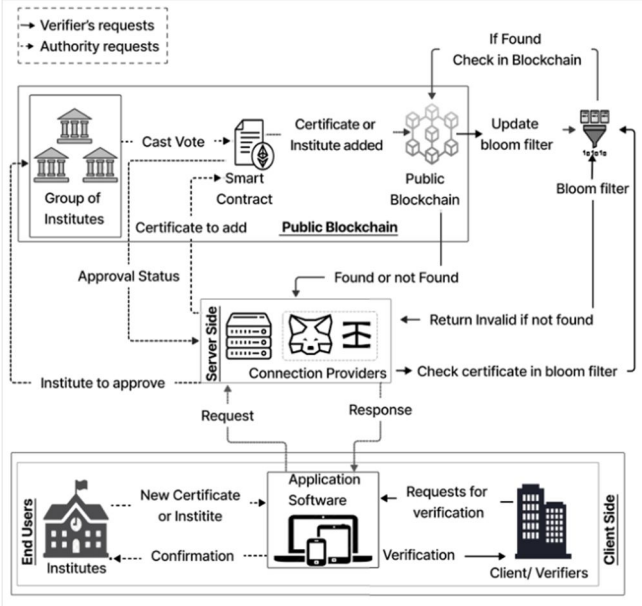


FIGURE 1. Architecture of certificate verification system

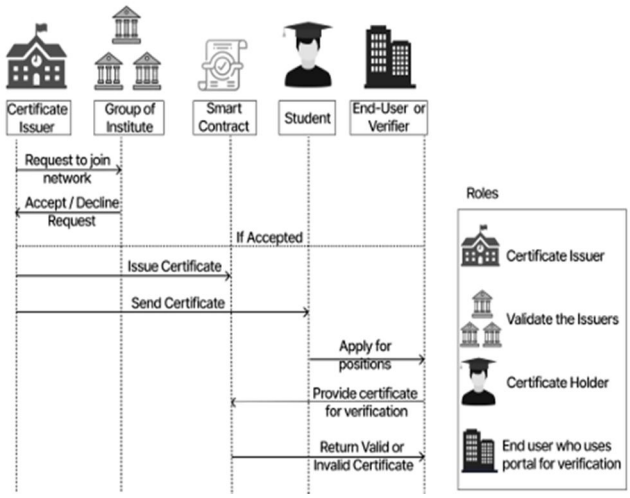
A. System Overview

Running in a blockchain network, where all the transactions related to the certificate are stored in a tampered resistant distributed ledger, the system. It combines Ethereum smart contract, cryptographic hashing, and a Bloom Filter-based pruning mechanism to provide secure and efficient certificate verification. In contrast to centralized model, our proposed method diminishes the significance of single authority, and rather, significant amount of trust is distributed among multiple known and verified entities.

B. System Architecture

The architecture of our proposed system can be defined through four main entities:

1) *Validator:* Trusted entities that keep the blockchain network and take part in validating new entities through a voting process.
2) *Certificate Issuer*: Accredited bodies that issue certificates to users. Trusted certificates can only be generated by verified issuers.
3) *Certificate Holder:* Receives certificate and submits it for verification on demand.
4) *Verifier:* A company or entity which validates certificates authenticity using the system. These agents communicate with one another via a front-end that interfaces with the block-chain back-end, allowing for a smooth communication layer and a secure data exchange.



Certificate validation process by the verifier organization.

C. Working Mechanism:

The proposed methodology operates through a workflow and works as follows:

1) *Institutional Registration:* New institutions apply for network access. The existing validators validate the request by a consensus-based voting process. Trusted issuers are only the registered banks, the certifying bodies.
2) *Issuing a certificate:* When a certificate is issued by a trusted authority, its information is hashed with double SHA-256. This hash works as a unique identifier and is saved on the blockchain through smart contracts.
3) *Bloom Filter Update:* The derived hash is also mapped into a Bloom Filter data type which provides a quicker search on verification round.
4) *Certificate Storage:* The hashed credentials are written into the blockchain, which provides immutability and prevents tampering of the record.
5) *Certificate Verification:* On presenting a certificate to the verifier, the verifier performs the same hash on the certificate and checks the Bloom Filter. Negative results mean the certificate is discarded right away. If it is positive, final verification is done against the ledger using smart contracts.

D. Smart Contract Functionality:

Smart contracts assist in automating the systems operation. The primary functions are:

Add Certificate:	Records the certificate hash to the blockchain.
. Verify Certificate:	Checks whether the certificate is authentic by comparing its hash value.
Add Institution:	Adds a new institutions in the network.
Vote:	Enables validators to approve or disapprove new institutions.

These automated operations decrease the need for human interaction, and increase the dependability of the application.

E. Security Properties

The suggested scheme includes several security features:

1) *Immutability:* Blockchain ensures that once data is written it is never modified.

2) *Data integrity:* SHA-256 hashing makes any modification in certificate data evident.
3) *Decentralization:* There is no single point of failure and trust is boosted.
4) *Resistance to Attacks:* We design the system to defend against Sybil and 51% attacks by means of limited validator participation and our consensus protocol.

F. Benefits of the Proposed System

The above advantages make the ultimate system proposed in this work significantly better than the state-of-the-art.
Tamper-proof certificate authentication is available
Decentralized and transparent verification is guaranteed
Cuts down the time of verification with Bloom Filter optimization
Minimizes the cost for operation of the efficient smart contract
In general, the proposed system provides a robust, secure and efficient mechanism for certificate authentication that overcomes significant challenges of traditional and current blockchain-based systems.

VI. SYSTEM ARCHITECTURE

Our proposed system employs a decentralized blockchain-based architecture that provides secure, transparent, and efficient certificate verification. The architecture is made such that frontend user activities are integrated directly with a blockchain-based backend to facilitate communication between the system entities where the data are made tamper-proof.

A. Architectural Overview:

The system has two main layers:
1) *Front-End Layer:* This segment will give all participant a live interface to work with the system. It enables institutions to issue certificates, certificate holders to retrieve their credentials, and verifiers to check the validity of certificates. The interface was designed to be user-friendly and to connect the end-user with the blockchain network effortlessly.
2) *Blockchain Back-End Layer:* The back-end is formed by the Ethereum blockchain network, where all the operations related to the certificates are carried out using smart contracts. It owns a distributed ledger that is provably secure to store certificate hashes. The backend also incorporates a Bloom Filter-based scheme for enhancing search efficiency.

B. Core Components

The architecture incorporates the following critical components:
1) *Smart Contracts:* Smart contracts: Smart contracts enable completion of certificate issuing, verification and institutional validation processes. They guarantee all operations to be performed safely with no human intervention.
2) *Blockchain Network:* It is a distributed ledger, where every transaction, the certificate hashes, and the validation logs, along with metadata are recorded, making it possible to maintain a trusted data source.
3) *Bloom Filter Module:* A probabilistic data structure to enhance search efficiency, since it can be used to know quickly if a certificate is not in a queried blockchain.
4) *Cryptographic Hashing (SHA-256):* Used to generate unique hash values for the certificate data which provides security and privacy when certificate data is shared.

C. System Entities

The architecture consists of four major components:
1) *Validator:* "Good guys" (e.g., banks) who maintain the network and vote on which new institutions get to join.
2) *Certifier:* recognized entities that issue certificates on the blockchain.
3) *Certificate Holder:* The person to whom the certificate is issued who can be used for verification.
4) *Verifier:* Entities like banks who use the system to verify certificates.

D. System Architecture:

Data Flow
The system operates according to a structured data flow:
Institutions have their certificate data to be submitted through the front-end page.

The data is hashed by using SHA-256 and then sent to the smart contract.
The smart contract stores the hash on the blockchain.
The hash is inserted in the BF, to make query runs faster.
When a query is verified, the BF is tested prior to the blockchain query.
The interface returns the result to the verifier.

E. Feature of architecture

1) Decentralization: Removes reliance on central authority
2) Immutability: Guarantees data cannot be changed after stored
3) Efficiency: Shortens verification time by using Bloom Filter enhancement
4) Security: Data is secured with hashing and consensus
5) Scalability: Backed by large scale certificate verification infrastructure

In summary, our architecture enables a strong scalable solution for secure certificate authentication that overcomes the performance and security obstacles found on today's digital system

VII. ANALYSIS OF RESULTS

The efficiency of the proposed blockchain based certificate authentication system is evaluated with respect to the transaction cost, certificate verification time and the overall system efficiency. The analysis confirms that how smart contract and Bloom Filter optimization integration contributes to the system performance.

A. Transaction Cost Analysis

The price of performing operations on the blockchain network is denominated in the gas. Each smart-contract function, e.g., add certificate, verify certificate, and register a new institution, has a fixed gas cost.
The total transactional cost is a function of gas consumption and gas price in the Ethereum network. The experimental results show that the cost of including a certificate is comparatively inexpensive as opposed to conventional blockchain based systems. Though the cost of adding a new institution is marginally higher, it is a one-off procedure and it has little to none impact on the performance of the system as a whole.
The results show that the proposed system achieves a good performance/price ratio, thus it may be deployed at large scale in scientific and professional communities.

B. Certificate Verification Time

Certificate verification time is a significant quality metric. The system considers two cases for evaluation purposes:
True Case (Certificate Exists): When the certificate is actually in the blockchain the system checks the Bloom Filter, and then goes to the blockchain for a final check. There is a small overhead, because an additional Bloom Filter step is added.
False Case (Certificate not existed): When certificate does not exist, the Bloom Filter efficiently detects the no-existence, and then the verification ends without accessing the blockchain.
The results demonstrate that the proposed method can greatly reduce the verification cost in the false case, which is critical in a practical environment because number of invalid or non-existent certificates can be expected to be large. The delay is negligible for the true case, for the great speedup in the false case is well worth it.

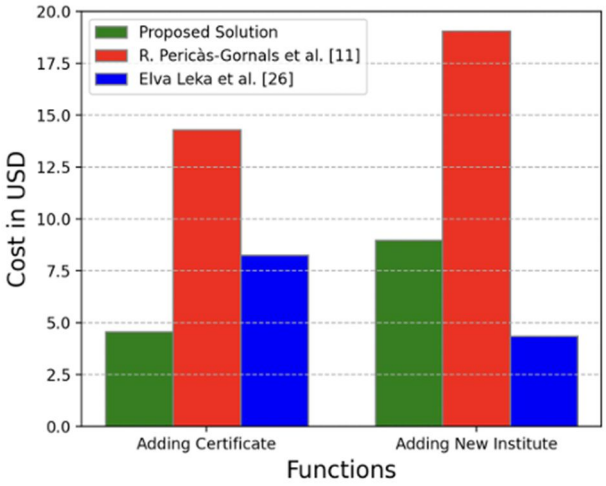
C. Efficiency Improvement

By introducing Bloom Filter, system efficiency is improved as it avoids unnecessary querying to the blockchain. This optimization works especially well for large systems so many verification requests are sent per unit time.
The proposed system outperforms the traditional verification method and the existing blockchain solution in terms of response time and scalability.

D. Security and Reliability Analysis

The system has achieved reliability and security through multi-mechanisms. Blockchain immutability ensures that a certificate, once posted, cannot be changed.

The use of SHA-256 hash assures data integrity while the decentralized model eliminates single points of failure. The consensus-based system of validation also mitigates the potential risk of an unauthorized organizations issuing certificates, which could lead to fraud. Further, the system can withstand standard blockchain attacks such as Sybil and 51 % attacks in a provably strong manner even under adversarial setting.



Cost comparison with existing solutions.

VIII. SECURITY ANALYSIS

Security is an essential aspect for any certificate authentication system, more particularly when applied to sensitive academic or professional certificates. The designed blockchain-based approach provides a three-layer defence strategy to protect against data manipulation, guarantee the data source authentication, and mitigate common cyberattack threats.

A. Data Integrity and Immutability

It is based on the following principles: a hash function is used to ensure the data integrity. Each certificate is transformed into a unique hash value and then saved on the blockchain. any change in the certificate's data will produce a different hash, so it can be easily identified if there is any fraud. In addition, block chain technology creates an immutable environment, so a certificate, once recorded, can never be changed or erased. This ensures the permanence of the stored records.

B. Decentralization and Elimination of Single Point of Failure

The proposed architecture is different from the previously centralized systems and it executes on a decentralized blockchain network. Information is replicated to many nodes, rather than tied to a single point of failure. if a node goes down, even if it is compromised, the system as a whole still remain safe and capable of operation, which assures high availability and high trust.

C. Protection Against Sybil Attacks

A Sybil attack is an attack where one attacker masquerades as multiple nodes in the network. The system we propose addresses the problem of Sybil by once again allowing each institution just one verified identity on the network. New institutions also are subject to a consensus-based voting procedure by already trusted validators. This vetted admission process excludes unverified actors from entering the system.

D. Resistance to 51% Attacks

In blockchain systems, a 51% attack is an attack in which a single entity gains control over the majority of the network, such as hash rate or stake, and is able to but not totally control the transactions on the blockchain. The proposed architecture mitigates this threat through adoption of Ethereum's high throughput consensus mechanism alongside the diversification of control among several trusted organizations operating nodes. The need for collective validation and voting also makes it computationally and practically impossible for a single actor to take over the network.

E. Signed Secure Authentication with Digital Signatures

The mechanism operates using asymmetric cryptography in certificate authentication. Trusted organizations sign certificate hashes digitally with their own private key. At the time of verification associated public key is used to verify the signature. This makes certain that the certificates are only issued by trusted organisations and it's not tampered.

F. Privacy Preserving Data

To protect privacy, instead of recording the actual certificate data on the blockchain, only the cryptographic hash of the certificate is stored, in a manner similar to [29]. Since hash functions are one-way, it's unfeasible to decrypt the hash and get back the original certificate. It allows to keep sensitive data secret and still be able to verify.

G. Smart Contract Security

Smart contracts are employed to automatically issue, validate, and verify certificates. These contracts are written to minimize potential vulnerabilities by using secure-equivalent coding practices. Potential issues can be identified through the use of static analysis tools to make sure the deployed contracts are solid and reliable.

H. Overall Security Assessment

Cryptographic hashing, decentralized structure, consensus-based validation, and secure smart contracts collectively offer complete security assurance. The system protects well against data modifications, unauthorized data access, and well-known blockchain attacks with intelligence and high transparency.

IX. CONCLUSION

In this paper, we propose a secure and decentralized solution for the certificate authentication using blockchain technology, which overcomes the drawbacks of centralized approaches for certificate verification. The system exploits Ethereum smart contract and SHA-256 cryptographic hash functions to provide proof-of-existence, integrity and process transparency. By removing the dependence on centralized entities, the proposed method increases trust and eliminates the potential for data tampering or unauthorized access to data.

One of the contributions of this work is the combination of the BF-based search optimization technique to improve the verification performance by preventing unnecessary queries to blockchain. This is an important efficiency optimization, especially in big-scale system that need to validate much certificates very quickly. In addition, the consensus-based voting scheme enhances the accountability of the system, as it does not allow a single entity to issue valid certificates but rather only a trusted institution can do so.

The performance evaluations show that our solution can offer reduced transaction cost of certificate operations and accelerated certificate verification, particularly in the case of invalid certificates. The scheme is also demonstrated to be resilient to popular blockchain attacks including Sybil and 51% attacks, which guarantees the reliability and security. In summary, the proposed technique can be a scalable, cost effective and secure way for certificate authentication. To summarize, the protocol improves transparency, efficiency and trust with respect to educational institutes, employers and certificate holders which makes it a working solution for real world application.

X. FUTURE WORKS

Although the blockchain-based certificate authentication scheme proves to be secure, transparent, efficient and feasible, there are still some issues to be further improved to enhance its functions and applicability in the real world.

To begin with, scalability can be enhanced through the introduction of advanced block chain solutions, such as Layer-2 protocols and sidechains, which enable the processing of much higher numbers of users and transactions with lower latency and cost. This would make the system better suited to be used on a national or global basis.

interoperability enhancing by producing standard API, middleware to enable plug and play integration with architecture of institutional database, recruitment platforms and government systems. This would permit the interoperability needed for common networked applications and boost usage.

It may also be applied to multi-domain certificate verification, which includes professional certification, health care records, and government-issued documents. That would also widen the system from purely academic use.

Using more sophisticated cryptographic primitives such as zero-knowledge proofs may introduce additional privacy enhancement as it allows to verify without disclosing secret information. It would bolster data privacy while maintaining transparency.

Future work might also include optimising smart contract execution to decrease gas usage and operational costs making the system less costly to run for institutions with a small resource base. the seamless integration of easy-to-use mobile and web apps with the underlying infrastructure can enhance the experience and convenience for certificate holders and verifiers. Among these are features like QR code-based verification and real-time validation that can further improve the experience.

Lastly, testing and deployment in partnership with schools and organizations may yield insight into performance and usability of the system for continual improvement and refinement.

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. R. 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 Journal on Information Security, vol. 2021, no. 1, pp. 1–9, 2021.

[3] A. Tariq, H. B. Haq, and S. T. Ali, "Cerberus: A Blockchain-Based Accreditation and Degree Verification System," IEEE Transactions on Computational Social Systems, 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," Journal of Medical Systems, vol. 43, no. 1, pp. 1–9, 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 of Things and Cyber-Physical Systems, vol. 3, pp. 309–322, 2023.

[6] K. Christidis and M. Devetsikiotis, "Blockchains and Smart Contracts for the Internet of Things," IEEE Access, vol. 4, pp. 2292–2303, 2016.

[7] R. Pericàs-Gornals, M. Mut-Puigserver, and M. M. Payeras-Capellà, "Highly Private Blockchain-Based Management System for Digital COVID-19 Certificates," International Journal of Information Security, vol. 21, no. 5, pp. 1069–1090, 2022.

[8] S. Mondal, A. Panja, and S. Karforma, "An Efficient E-Certificate Management System in E-Learning Using Blockchain," Science and Culture, vol. 89, nos. 3–4, pp. 1–5, 2023.

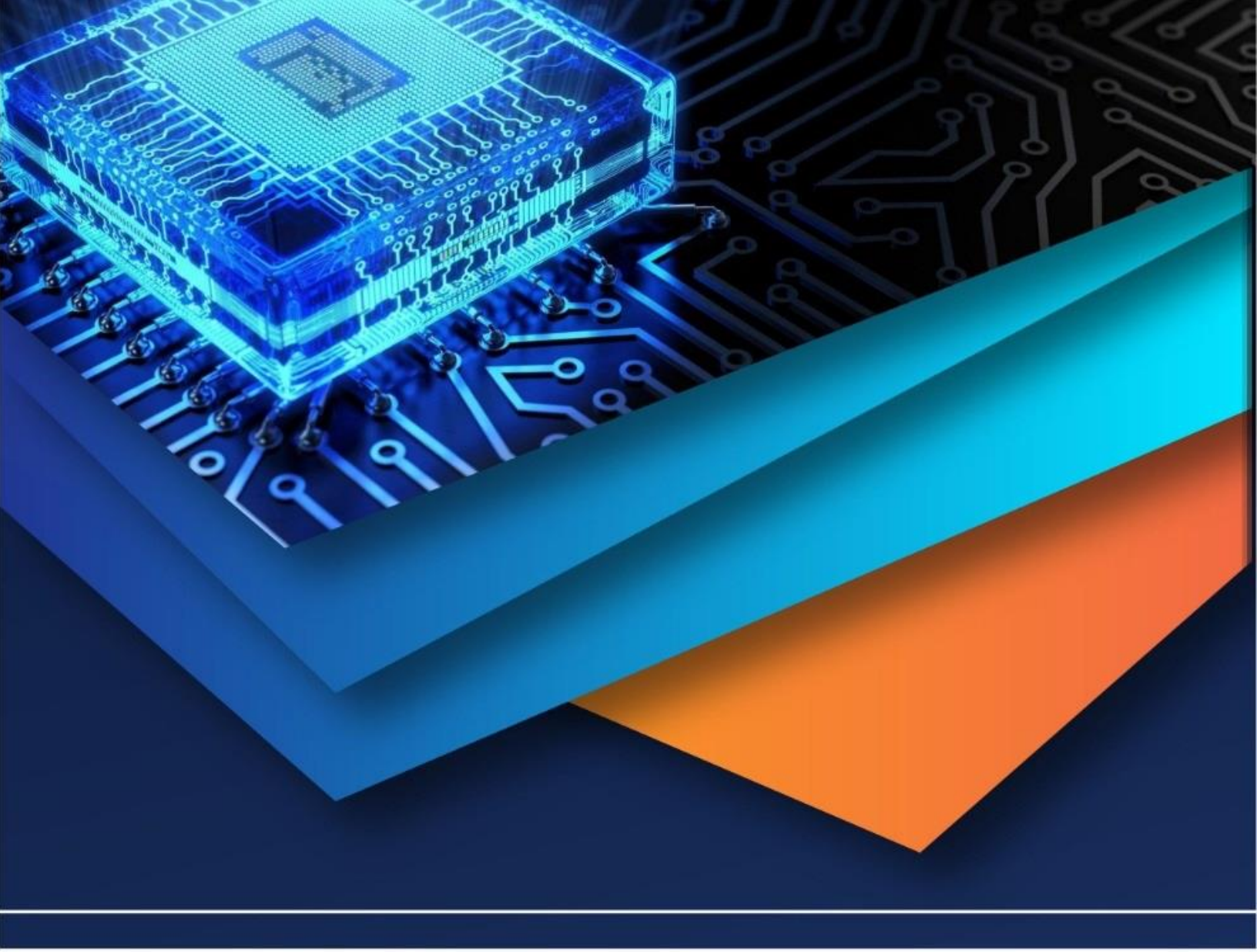
[9] A. Garba, Z. Chen, Z. Guan, and G. Srivastava, "LightLedger: A Novel Blockchain-Based Domain Certificate Authentication and Validation Scheme," IEEE Transactions on Network Science and Engineering, vol. 8, no. 2, pp. 1698–1710, 2021.

[10] 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.

[11] R. F. Ghani, A. A. Salman, A. B. Khudhair, and L. Aljobouri, "Blockchain-Based Student Certificate Management and Sharing Using Hyperledger Fabric Platform," Periodicals of Engineering and Natural Sciences, vol. 10, no. 2, pp. 207–218, 2022.

[12] R. Priyadarshini et al., "A Faster, Integrated, and Trusted Certificate Authentication and Issuer Validation System Based on Blockchain," IEEE Access, vol. 13, pp. 27037–27047, 2025.

[13] J. Feist, G. Grieco, and A. Groce, "Slither: A Static Analysis Framework for Smart Contracts," in Proc. IEEE/ACM Int. Workshop on Emerging Trends in Software Engineering for Blockchain, 2019, pp. 8–15.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY