International Journal of Scientific Research & Engineering Trends
Volume 12, Issue 2, Mar-Apr-2026, ISSN (Online): 2395-566X

Blockchain Based Certificate Management and Verification System

1st Jayashree Pasalkar, 2nd Vedant Mahanavar, 3rd Pranav Patil, 4th Om Mahajan
Department of Information Technology, AISSMS Institute of Information Technology, Pune, India

Abstract- — Counterfeit academic certificates have increased sig- nificantly enough so they now create problems for many organiza- tions (i.e., schools, employers, government agencies) because they reduce faith in the ability of organizations to verify credentials. Most current methods used to manage academic certificates are primarily manual and/or based on centralized database storage; therefore, most are subject to various forms of manipulation (e.g., unauthorized access/modification), delayed processing, and additional risks associated with verification processes. Blockchain technology has recently emerged as a possible solution for authenticating certificates securely; however, many of the current blockchain implementations are built upon platforms such as Ethereum, which experience both high transaction costs, and limited scalability. To overcome these constraints, this research will present a blockchain-based certificate management and verification system that utilizes the high-performance and low cost attributes of the Solana blockchain platform with a Django- based backend system. With this system, academic institutions can issue certificates (while maintaining the original formatting), or register external certifications issued to students/alumni. All generated certificates are hashed using the SHA-256 hashing algorithm, and each unique hash is stored on the Solana blockchain via a Rust-based Anchor smart contract. Upon receipt of a certificate to be verified, the proposed system hashes the submitted certificate, and then compares its hash value with the unalterable blockchain record to authenticate/verify the legitimacy of the submitted certificate, or identify if the submitted certificate was altered/tampered. In combination with the security provided by blockchain, the scalability of the Solana blockchain, and an efficient backend architecture, this proposed system provides a highly effective method of verifying the authenticity of academic certificates, while reducing the risk of fraudulent activity.

Index Terms—Blockchain Technology, Certificate Verification, Smart Contract, Solana Blockchain, SHA-256 hashing, Decen- tralized Credential Management, Django Framework.

I. INTRODUCTION

In academic life, you study for years to earn degrees and in your professional career, you work hard to receive certificates that support your journey toward success. These papers are widely used for admissions, hiring and professional certifica- tions. But the increase in fake and forged certificates has turned into a major headache for schools, businesses and government agencies around the world. This drives more people to use fake credentials which, while decreasing such data verifiability and fidelity, also harms the integrity of authentic institutions as it can have cascading effects on economy and esteem.

Most existing certificate management and verification sys- tems are centralized, and depend on either issuing institutions or a third party intermediary to do manual verification. These are not very effective systems, and are quite easily forged and modified without approval. Additionally, storing certificate records in centralized databases can cause issues such as data tampering, single points of failure and lag time when verification is requested. These limitations indicate that we require a secure and public method that still provides certificate authenticity without losing usability and performance.

In the recent past, blockchain technology has emerged as a potential method to securely store data and validating it through decentralized means. Using a blockchain is a reliable method of ensuring the correctness of data on the one hand and, on the other hand, preventing people from changing this data without permission due to its immutable and decentralized nature. Several blockchain-based certificate verification solu- tions based on Ethereum and Hyperledger Fabric have been developed. These algorithms utilize the decentralized nature of blockchain, yet encounter issues such as high transaction fees, limited scalability, and network overload. Those constrictors can make them more difficult to put into practice, especially in sensitive areas where cost-effectiveness and performance are critical.

This paper introduces a blockchain-based certificate man- agement and verification system based on Solana blockchain and Django-based backend infrastructure to overcome these

challenges. According to the proposed framework, certificates may therefore be issued natively within the system or registered directly from external sources while retaining their original format. Each certificate is processed through the SHA-256 cryptographic hashing algorithm, and a Rust-based Anchor smart contract securely stores the resulting hash on the blockchain. The verification process recalculates the hash of the certificate that has been submitted and compares it to the immutable record held on the blockchain in order to check its authenticity, identify any modifications. The proposed system uses Solana's high throughput and low transaction costs to make certificate authentication more scalable and efficient, without the need for third-party middlemen.

The remainder of this article will be organized per the following system. Section two shall encompass the literature review related to blockchain-supported methods of validating documents. Section three will be an analysis of the architecture and methodologies of the proposed system. Section four will discuss the testing of the proposed system and potential success of the implementation. Section five will present the advantages and disadvantages, challenges, and trade-offs as- sociated with using this approach. Finally, Section six will conclude this paper and provide specific recommendations regarding future studies in this field.

Both professional and academic certification serve as significant formal documentation of the qualifications of an individual; therefore, issuance of formal documentation demonstrates an individual's level of education, skills, and abilities associated with a specific job position. Formal documentation is commonly used in attaining employment, college admissions processes, and/or attaining professional licensure and/or certification. As the incidence of false formal documentation has increased globally, verification of the validity of an individual's formal documentation has become a larger issue for all parties involved with the issuance of formal documentation; however, it may also present challenges for a regulatory agency responsible for overseeing the quality of education and formal certification within the job market. The consideration of negative economic results caused by the issuance of false formal documentation is also possible.

Traditionally, the predominant method used for certificate management and verification has been centralised systems, which have relied on a combination of both institutionally generated certificates and third parties for manual verification. Unfortunately, these systems are also inefficient and easily forged, as all certificates are able to be modified without limitation. In addition to the limitations associated with the efficiency of these two systems, a centralised database storing certificate records additionally subjects an organisation to data manipulation and has the potential to create a single point of failure. Furthermore, delays are likely when an organisation is verifying certificates. Therefore, there is a need for more secure and transparent methods for verifying the authenticity of certificates, as well as maintaining both efficiency and accessibility.

Blockchain technology has developed into a popular, secure means to store data and verify data without using a centre of verification since the emergence of decentralized systems. Blockchain allows for immutability and distributed data across multiple parties in a single system, thus ensuring the integrity of the data and preventing any unauthorized change to the information stored on a blockchain. To leverage the benefits of blockchain's decentralized architecture for certificate verification solutions, there have been multiple implementations of certificate verification solutions using various blockchain platforms including Ethereum and Hyperledger Fabric. When compared to traditional certificate verification systems, the use of blockchain will provide the benefits of decentraliza- tion; however, certificate verification solutions continue to be plagued with several challenges including, but not limited to, high transaction fees, limited scalability, and network congestion. These limitations will restrict the practical implementation of these solutions, especially in the environments where efficiency and performance are paramount.

In order to address these current limitations, we present a novel blockchain-based certificate management and verifica- tion system utilizing the Solana blockchain upon which we build a Django backend infrastructure for certificate issuance and/or registration from external sources retaining their origi- nal format; all certificates will be processed using SHA256 as the cryptographic hashing algorithm and the resulting hash will be securely stored on the blockchain via a Rust programmed Anchor Smart Contract. The verification process involves the system to recompute the hash of the provided certificate and compare that computed hash with the immutably stored hash on the blockchain to authenticate the certificate and identify any alteration. The system is built to leverage the high throughput and low cost associated with transactions made on the Solana blockchain and thus provides a high-performance, cost-effective solution for authenticating certificates in a scalable manner without relying on third party intermediaries.

This paper is structured into the following six sections. The second section will provide a literature review on certifi- cate verification systems using blockchain technology. Section three covers the proposed design and approach of the system. In section four we will examine how the proposed system will be

evaluated and anticipated performance. In section five, the discussion of implications, challenges, and trade offs of the proposed design will occur. Lastly, the last section includes the conclusion and potential areas for future research.

II. RELATED WORK

A. Blockchain-Based Certificate Verification Systems

Functioning with blockchain technology in this regard has become a huge option for ensuring that the certificates are verified authentically and have not been tampered. Due to its decentralized and immutable characteristic, the method is applicable in controlling academic credentials without third party [4],[5].

Vikhankar et al. Makmud et al.[1] proposed an Ethereum- base electronic certificate verification system where certificates are issued by smart contracts and stored as cryptographic hashes on the blockchain. Using a web-based interface, insti- tutions can issue, verify and revoke credentials in this system, which helps ensure transparency and reduce the potential for forgery of certificates.

In a similar work, Gangwar and Chaurasia [2] proposed a blockchain-based certificate authentication system with de- centralized storage and verification mechanisms. Their system uses QR codes along with blockchain to allow fast and efficient certification validation.

Hasan et al. [3] proposal presented DistB-CVS, a dis- tributed blockchain-based certificate verification system for environments that restrict the usage of public cryptocurrency. It specializes in facilitating the secure verification of data within distributed nodes, ensuring both integrity and authenticity.

Other scholars have focused on the use of blockchain for verifying documents and credentials. For example blockchain-based document verification systems, which can provide se- cure and tamper-proof validation of digital records and cer- tificates [6], [7]. Such systems demonstrate a way to use blockchain to increase authenticity and verity in document verification.

Rustemi et al. In their work [4], a systematic literature re- view about blockchain-based certificates verification solutions was conducted and the proposed ones were classified accord- ing to the anchored types: functionality, scalability, efficiency and interoperability. Likewise, said et al. — [5] introduced a comprehensive study of the blockchain technology enabling architecture and security perspectives.

Additionally, the restitution research of consensus mech- anisms in blockchain has also increased the reliability of blockchain systems. Consensus algorithms have had extensive commercial exploration, providing data integrity and fault tolerance in distributed networks [8].

B.Limitations of Existing Blockchain Solutions

Although moving verification to a blockchain-based system does provide improved security and transparency, it is not without its problems. For solutions, the emphasis is heavily on the Ethereum blockchain; during congested periods with gas fees this translates into high transaction costs. [1], [2]

On the other hand, due to the timeliness of development, they are deeply rooted in Ethereum only 15–45 transactions per second machines will cause organizations certification applications and verifications like everything is a wireless trouble. [8] Therefore such systems are difficult to adopt by large agencies because they are not able process that many certificates during a transaction.

As for the safety, it is also a problem in many blockchain- based systems. Bonnie exposit, small to report on to ability. GDPR compliance is not enough in its own right for safe- guarding your data when it is not in use Storing complete certificate data on the public blockchain might expose sensitive information to others if it is not protected by some alternative remedy such as trusted computing systems or secure multi- party computation [6]. Several innovations try to avoid doing so via either offline storage and mixed-edge technologies, or some hybrid approach that combines multiple methods.

Institutional environments can use permissioned blockchains like Hyperledger Fabric to achieve access control and greater efficiency. However, this solution fails to provide the same degree of openness or even verifiability available with truly open blockchain networks; it thus has little application in chinese baby stroller production verification engineering[4].

C. Comparison of Existing Approaches

Table I, we present a high-level overview of the state of blockchain-based certificate verification systems and their key limitations. However, existing solutions tend to rely on Ethereum-zation-based archetypes that afford secure certifi- cate storage but are encumbered by performance sins and prohibitive operational costs.

Table I
Comparison Of Existing Blockchain-Based Certificate Verification Systems

System	Blockchain Plat-form	Key Limitations
Vikhankar et al. [1]	Ethereum	Smart contract-based certifi- cate verification but does have high fees for transaction while there is network congestion.
Gangwar & Chaurasia [2]	Ethereum + IPFS	QR-code for authentication along with decentralized storage and limitation for scalability.
Hasan et al. [3] (DistB-CVS)	Private Blockchain	Decentralized verification Of certificate with no public cryp- tocurrency, but no public trans- parency.
Ethereum-based Systems	Ethereum	Limited scalability with 15-45 TPS and gas costs affecting large-scale certificate issuance.
Proposed System	**Solana**	High throughput and low transaction cost with secure hash-based certificate verification.

Alright, so to deal with this problem newer blockchains like Solana have been developed which promise upto a much higher transaction throughput and lower transaction cost. A hybrid architecture using the Solana blockchain and a Django backend. It keeps only the cryptographic hash of on-chain certificates while keeping certificate data off-chain. By doings so, it allows for better scalability, reduced cost and increased privacy while providing tamper-free certificate validation.

III. SYSTEM DESIGN AND IMPLEMENTATION

The blockchain-based management of certificates proposed in this linked to the verification system aimed at providing secure, scalable and valid mechanism to issue and verify academic credentials. The general structure of the overall architecture is that it has a web-based interface, a backend pro- cessing layer and the Solana blockchain network for tamper- proof storage and verification. Training Data Preprocessing: The system uses a hybrid architecture in which certificate metadata is off-chain while the corresponding cryptographic hashes are placed securely on the blockchain.

The proposed system architecture is shown in Fig. 1. Overall, the system has several major components frontend interface, Django backend services, Decentralized Verification and Blockchain Interaction Module mechanism. By combining these components, secure certificate generation, storage, and authentication.

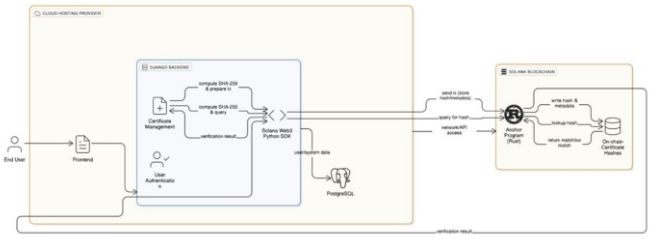

Fig. 1. Enter Caption

A.User Interface Layer

The main interaction with user through UI layer. It enables permitted organization software programs to create new help systems and external customers including companies or a certificate authority to manually verify certificates. In addition to visiting our web interface, users are able to upload certificate data or type the certificate identifiers for verification. This interface is responsible for sending requests to the backend server and obtaining verification results.

B.Backend Processing Layer

The backend layer is developed by using the Django framework to allow system operations, authentication and communication with the blockchain network. This layer deals with certificate registration, certificate management and verification requests. For example, upon issuing/registering a certificate the backend does some processing with the certificate data and generates a cryptographic hash on SHA-256 hashing algorithm. The backend also stores user records and system metadata in a relational database like PostgreSQL. This helps reduce storage costs and leave an event with only cryptographic fingerprints of off-chain data while acting as a solution to improve performance without compromising security.

C.Blockchain Interaction Layer

The Solana Blockchain Interaction layer acts as a bridge between the backend application and Solana blockchain network. This module uses Solana development tools and libraries to send transactions to the blockchain. The storage of certificate hashes and verification logic is managed through a smart contract implemented with the Rust-based Anchor framework. The generated SHA-256 hashed value is sent through a transaction to the blockchain at time of issuance and stored as an unalterable record. In verification, the system checks against the blockchain if such certificate hash exists and
verifies that it corresponds to the submitted certificate.

D.Certificate Verification Mechanism

The entity that verificar the certificates means it is still complete and verifications. The SHA-256 hash of the certificate file is then recomputed and compared with the hash on the blockchain when a certificate is submitted for validation. When the hashes match, it proves certificate is valid and has not been tampered. When the hashes are compared, and they do not match: The system flags the certificate for being invalid or potentially modified.

By allowing employers, organizations or other stakehold- ers to verify educational achievements instantly, this process removes a huge burden from issuing institutions in terms of manual verification.

IV. SYSTEM IMPLEMENTATION AND METHODOLOGY

To address this gap, we develop a prototype of the proposed blockchain-based certificate management and verification system using a hybrid architecture that consists of a backend developed in Django alongside the Solana blockchain network. Using cryptographic hashing and decentralized storage in a manner that is sufficiently on-chain efficient; the implementation aims to go beyond simple stability by providing unprecedented levels of certificate integrity, authenticity and verification.undefined Its whole workflow can be divided into three steps: issuing the certificate, storing its hashes on-chain and verifying the certificate.

A.Certificate Issuance Phase

The process for issuing a certificate begins when an authorized issuer logs into the system via the web-based interface. Certificate attributes such as student details, course information, certificate identifier and completion date are entered by the issuer. These inputs are sent out to the backend server and organized into a structured data which can be used in later stages.

The certificate file data is then prepared and a hash of this data using the SHA-256 hashing algorithm is generated. The hash is uniquely representative of the content of the certificate such that even a slight change in the data present will produce a completely different hash value. This is then used to generate the hash which becomes the key identifier for the certificate on blockchain.

Once hash is generated, backend builds a blockchain transaction with the certificate hash and not much else, like issuer identity and timestamp metadata. It is then signed with the issuer's blockchain wallet credentials for legitimacy and responsibility, before being sent out onto the Solana network.

B. On-Chain Certificate Storage

Once the transaction is received on the Solana network, it gets processed by a smart contract written in the Rust- based Anchor framework. The smart contract keeps track of all certificate records and stores the generated hash in a structured blockchain account.
Every certificate record stores the certificate hash, issuer's public key, and the timestamp at which it was issued. The

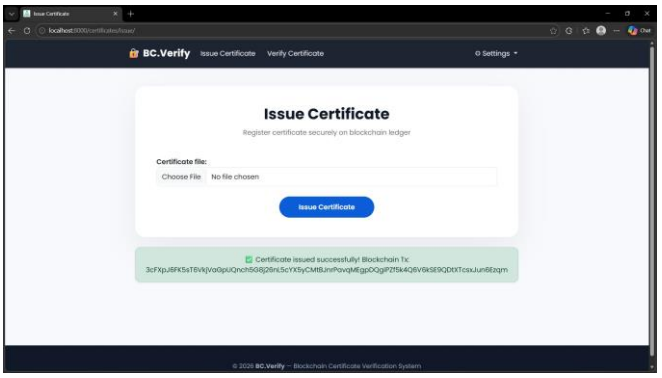

Fig. 2. Enter Caption

system saves money on storage, and to be efficient, it only stores the cryptographic hash on the blockchain while storing the complete data about the certificates off-chain.

A traditional relational database like PostgreSQL stores off-chain certificate metadata and document references. The identifier for the transaction is recorded along with the corresponding database representation, so long as users of this system can always retrieve all relevant information about a certificate without modifying the original record on blockchain.

C. Certificate Verification Workflow
It enables third parties (employers, institutions, verification authorities) to validate the authenticity of that particular certificate At the time of verification, During the verification process, the user will either upload a certificate file or provide a certificate identifier via the actual verification interface.
The backend system performs SHA-256 hashing of the user-submitted certificate data again and invokes the blockchain smart contract to check if this corresponding hash exists in the blockchain records. The hash, obtained from rehashed certificate data, is then compared with the blockchain hash already stored in the system.

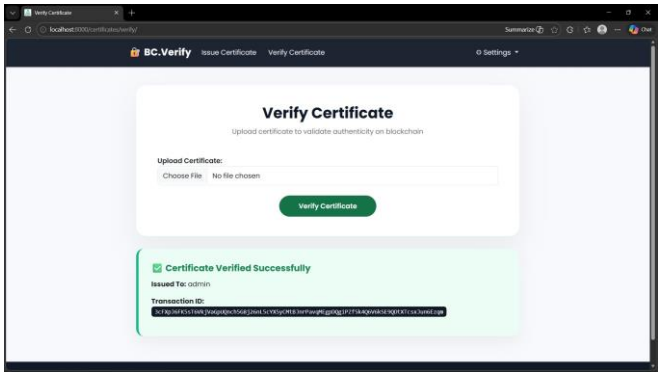

Fig. 3. Enter Caption

If hashed values in the newly generated data does not match with record stored on blockchain or failed to find a record of it, then the certificate is said to be invalid or potentially

tampered. They also supply blockchain transaction specifics seen via a blockchain traveler for the function of transparent and verifiable verification that the certificate document was generated.

D. Certificate Verification Workflow
Employers, institutions, or other stakeholders can verify the authenticity of a certificate through the verification process. During verification, the user either uploads the certificate file (e.g..pfx; if applicable) or enters the certificate identifier in a request sent to the verification interface.

The backend restructures the SHA-256 hash of their sub- mitted certificate and matches it with its related hash stored on blockchain. Whether the computed hash matches the record in the blockchain — if true,Means that the certificate has not changed, it is authentic. When they do not match, the system marks the certificate as invalid or potentially altered.

Algorithm 1 details the process of certificate issuance and its registration on blockchain in the proposed system.

Algorithm 1 Certificate Issuance and Blockchain Registration
Require: Certificate attributes D
Ensure: Certificate hash stored on blockchain
1: Certificate details D are inputted by issuer via web inter- face
2: The backend translates certificate data to JSON
3: Calculate SHA-256 H of data in certificate
4: Build H containing transaction for the blockchain
5: Using the issuer's wallet credentials, sign the transaction
6: Issue transaction to solana network
7: Off-chain database storing certificate metadata
8: Associate database record to blockchain transaction ID

Algorithm 2 describes the certificate verification process in the proposed system

Algorithm 2 Certificate Verification Procedure
Require: Certificate file C
Ensure: Verification status (Valid / Invalid)
1: Extract certificate data from C
2: Convert and serialize the certificate into data
3: Calculate Hc, a SHA-256 hash of the certificate data
4: Issue a proof request with blockchain smart contract for stored hash Hb
5: if Hc == Hb then
6: Return "Certificate Valid"
7: else
8: Return "Respond with Certificate Invalid or Tampered"
9: end if

V. EVALUATION AND EXPECTED RESULTS

Because the proposed system is still in design and implementation, this evaluation was based on theoretical performance metrics inferred from architecture design and public benchmarks of Solana blockchain network. The metrics chosen

for evaluation are transaction throughput, cost of a transaction, security and scalability, which are primary considerations in the context of a system.

The first advantage of the proposed system is that the Solana blockchain provides a large transaction throughput. Solana supports thousands of transactions every second and has a peak performance of about 2,000 to 65,000 transactions per second based on the health of the network. By contrast, Ethereum-

based systems usually allow 15 to 45 transactions per sec- ond. Such a substantial performance enhancement makes the proposed system capable to support high-scale operations of certificates issuance and verification without suffering from performance bottlenecks, therefore making it suitable for use by universities, certification authorities and large organizations with thousands of credentials managed.

Another significant advantage of the architecture is cost efficiency. Transaction costs on Ethereum networks can skyrocket during times of congestion, but are usually around $0.50 and $5.00 per transaction. By contrast, a Solana transaction usually costs extremely low fees (usually less than $0.001 per transaction). This reduction in operating cost is significant enough to render the system economically viable for institutions issuing high volumes of certificates.

SHA-256 cryptographic hashing algorithm is the main mechanism which secures the system. This also protects any attacker from changing certificate data, since a change will lead to a different hash because of the SHA-256 strong collision resistance and extremely low probability of hash collisions. Furthermore, Solana's innovative approach is fur- ther reinforced by its novel Proof-of-Stake (PoS) and hybrid Proof-of-History (PoH) consensus initiative which protect the network against Byzantine failures, ensuring rapid transaction validation on distributed nodes.

Also, the system has a hybrid storage architecture which wiseness for scaling. The on-chain part only saves the hash of the corresponding certificate, and all the metadata information is stored in a conventional relational database like PostgreSQL. This mechanism naturally allows to save storage space on the blockchain while keeping certificates records integrity and verifiability. It serves a high number of queries per minute and allows certificate data to be retrieved quickly for requests needing verification.

A second performance differentiator comes from Solana's Sealevel runtime environment, which is built for concurrent transaction processing. This allows multi-certificate verification requests to be processed in parallel, reducing latency compared to legacy blockchain networks where transactions are concatenated sequentially.

Table II compares the main performance metrics of Ethereum-based certificate verification systems with those that would be operating using the architecture in the proposed system based on Solana.

Table II
Comparison Of Ethereum And Solana For Certificate Verification Systems

Metric	Ethereum	Solana (Proposed)
Transactions per Second (TPS)	15–45	2,000–65,000
Average Transac- tion Fee (USD)	0.50–5.00	<0.001
Confirmation La- tency (ms)	5,000–15,000	~400
Privacy Model	Certificate data often stored on-chain	Only certificate hash stored on-chain

VI. DISCUSSION

A.Advantages of the Proposed System

Benefits of Our Approach To Certification Management and Verification Since the launch of Notaries services by an intermediary, central authorities become responsible to manage risk, thus a decentralized mechanism provides sev- eral benefits over traditional centralized certificate verification models. One of the key advantages is the implementation of Solana blockchain which provides orders of magnitude more transactions and much lower processing cost than other large volume blockchain technologies like Ethereum. This powerful system can effectively process thousands of certificate issuance and verification requests, so institutions that issue thousands of digital credentials are a great fit.

Use of cryptographic hashing to ensure integrity would also be a huge add-on for the proposed system. The further protects the content of the certificate by creating a SHA-256 hash value based on the certificate data and writing only this hash value to the blockchain, so that once there is any modification in its original content, it can be easily found. A single character change in the certificate data creates a vastly different hash value, which helps to indicate tampered or forged certificates on verification.

The hybrid storage architecture also improves the efficiency in the system. Rather than going on-chain with complete certificates, a single hashed representation is stored on-chain while full certificate metadata sits in an off-chain database e.g. PostgreSQL. This allows to offload much of the burden on blockchain storage requirements, while still providing many of

the benefits in terms of security and immutability which blockchain provide.

The importance of decentralized verification capability. Employers, institutions or other third parties can directly verify the certificates through the system without contacting the issu- ing institution. Automated verification reduces administrative work and significantly speeds up the issuance of credentials.

B.Limitations

The proposed system has many advantages; however, some limitations also exist for implementing the solution in real-world scenarios. The system must fit within an existing institutional certificate management environment—that is a

problem. The data formats of educational institutionsmay vary, along with the process utilized to issue certificates in them; subsequently more methods of standardization will need to be considered to allow for a blockchain-based system implementation.

A further limitation pertains to blockchain wallet manage- ment on the side of issuing institutions, i.e. As certificate issuance transaction must be signed with a blockchain wal- let, institutions should have robust private key storage and management practices in place. Incorrect key management might result in low security or the unauthorized issuance of certificates.

Moreover, the proposed system assumes user–blockchain network interaction with reliable network connectivity. If the internet infrastructure is insufficient, communicating with blockchain services may delay certificate verification. While this is relatively rare, there may still be system performance impacts in some scenarios.

Also, user uptake could be a real world problem. Employers/verification authorities that are not familiar with blockchain-based verification mechanisms will need a guide-book to use this system effectively To Conclude

C.Future Enhancements

The proposed system might be extended to support addi- tional features and improvements in future work. One possible improvement is a decentralized storage layer, similar to the InterPlanetary File System (IPFS), used for storing the document describing certificate. The former would cause the system to be even more centralized, while also reducing reliance on centralized storage infrastructure.

One more thing that can be done in order to strengthen and enhance education institutions is the building of networks of multi-entity credentials by various local universities and certification institutions on a common blockchain-based verification system. A cross-institution network would make it possible for credential providers to interoperate and verify the credentials of others.

The use of advanced privacy-preserving techniques like zero-knowledge proofs could also be investigated to enable sensitive certificate information while still allowing for ver- ification. “Users are then able to prove the validity of their credentials without showing all certificate information.

Future implementations might also come with more user-friendly verification interfaces and mobile based verification tools to make usage easier for employers and institutions.

In the grand scheme of things, such advancements have potential to improve the scalability, security and usability of certificate management systems using blockchain.

VII. CONCLUSION

Likewise, falsified scrolling academic buildings and skilled certificates have been actual test for education and placing job indeed placing it dangerous for educational organizations, employers and tweaking bodies. Traditional verification systems rely heavily on central databases, and manual validation

processes that are often inefficient, time-consuming to validate and prone manipulation. These limitations expose the need for secure, scalable approaches to digital credential verification.

We offered a system that connects the Solana blockchain with a Django-based backend architecture to manage and verify certificates. This framework requires that each certificate would be hashed based on the SHA-256 algorithm which would give us a unique fingerprint of an individual certificate which would be stored within a smart contract deployed to the blockchain. Only the hashed entries are stored on-chain, while the certificate metadata itself is kept in off chain storage which guarantees a good mix of security with privacy and a optimal use of the storage.

Solana Blockchain mainly provides high transaction throughput and low cost per transaction, better than legacy blockchain platforms like Ethereum. Therefore, the system can achieve large-scale issuance and verification of certificates without significant operational costs or network congestion. Additionally, the Proof-of-History and Proof-of-Stake consen-

sus mechanisms of Solana facilitate secure transaction verification and effective operational behavior from their systems.
The approach presented has potentials to provide solutions for honesty and transparency of certificate verification process, while having its own issues. In reality issuers would need to operate secure wallets for the certificates they issue and integrate with other local institutional systems, and also be accepted by employers as an ID/verification authority. As a result, such blockchain-based credential verification solutions need to address these factors.

We anticipate future work concentrating on the full-scale implementation of systems, information management for certificate documents by connecting and integrating with decentralized storage platforms, and adopting advanced privacy-preserving approaches like zero-knowledge proofs. Additionally, with the evolution of interoperable credential networks, open cross-institution certificate verification could work as a framework to enhance confidence in their digital credential ecosystems. This report finally concludes how the proposed system could use blockchain technology in enabling a secure infrastructure that can be used to verify certificates in a scalable and trustful manner.

Acknowledgments

The authors are heavily thankful to their project supervisor and faculty members for their expert guidance in providing knowledge, constructive criticism which helped the achievement of this report. Their comments and suggestions contributed greatly to the study's direction.

The authors acknowledge the support provided by their institution to establish the appropriate academic environment and offer necessary resources for conducting this research. Finally, the authors also thank anyone and everyone who dedicated their time and provided feedback during development of the proposed system.

REFERENCES

1. S. Vikhankar et al., "E-Certificate Verification Using Blockchain," IJERT, 2024.
2. S. Gangwar and V. Chaurasia, "A Faster, Integrated and Trusted Certifi- cate Authentication System Based on Blockchain," IJCA, 2024.
3. M. Hasan et al., "DistB-CVS: A Distributed Blockchain-Based Certifi- cate Verification System," 2023.
4. A. Rustemi et al., "A Systematic Literature Review on Blockchain-Based Systems for Academic Certificate Verification," IEEE Access, 2023.
5. H. Said et al., "A Survey on Blockchain Technology: Evolution, Archi- tecture and Security," Journal of Network and Computer Applications, 2022.
6. "Design of a Document Verification System Using Blockchain," 2023.
7. "Blockchain-Based Certificate Management and Verification System," 2024.
8. "Consensus Algorithms in Blockchain-Based Applications: A Survey," 2023.
9. "Blockchain-Based Academic Certificate Verification System," 2023.
10. "Blockchain Technology for Secure Digital Credentials: Architecture and Applications," 2022.