International Journal on Science and Technology (IJSAT)
E-ISSN: 2229-7677 ● Website: www.ijsat.org ● Email: editor@ijsat.org

Blockchain-Based Secure Document Verification System for Ensuring Authenticity, Integrity, and Transparency

Mrs. Geetha[1], Ms. Ashika M[2], Ms. Deepika P[3], Ms. Ganikarika M[4], Ms. Devadharshini D[5]

[1]Assistant professor Department of Computer Science and Engineering,
V.S.B Engineering College, Karur, Tamil Nadu
[2,3,4,5]Department of Computer Science and Engineering,
V.S.B Engineering College, Karur, Tamil Nadu

Abstract

As a result of increased nefariousness of fraudulent documents in the last decade, the ability to trust the verification of credible documents has never been more important. Traditional verification processes can be tedious, require too much manual effort, and are open to tampering. This research project will seek to facilitate the verification of credentials by creating a blockchain enhanced credential verification structure. Blockchains include a decentralized, transparent, public, and immutable ledger that can be used for both storing and verifying credentials, and certificates. An employer, university, or credentialing stakeholder, at any time will now be able to instantly verify a credential from a ledger search on the blockchain where the credential is immutable and shared in a credentialing blockchain ecosystem. A blockchain enhanced credential verification system, as proposed, will reduce administrative burden and costs, develop trust from credentialing stakeholder users, and diminish fraudulent credential opportunities. The use of smart contracts and crypto/blockchain methods and protocols will improve efficiency, speeds, and faculties of integrity in the credential verification process. This proposed work could be extended in a number of areas of inquiry beyond education, including that which goes to the verification of a credential for professional certification, and the academic credentialing to learners.

Keywords: Blockchain; Document Verification; Digital Credentials; Smart Contracts; Cryptography; Immutable Ledger; Fraud Prevention.

1. Introduction

Recently, the importance of credential verification for government, employers, and educational institutions has increased. Credential verification historically has used centralized databases, or paper-centered credentials. Validating credentials this way can be prone to fraud and/or tampering, slow processing times, and costly administrative fees. The rise of fraudulent degrees and certifications has created more need for a secure, transparent, and efficient system for credential verification. The problem with fraudulent credentialing has also been facilitated/supported by past credential verification methods.

Blockchain and distributed ledger technology (DLT) may offer some solutions to credential verification challenges. Information stored on a blockchain is decentralized and immutable. One information is written only to the ledger that information cannot be removed or manipulated, so a blockchain systems for credential verification is ideal for collecting and verifying sensitive information such as educational or work-related credentials. The use of smart contracts can facilitate validation of information verification automatically. With smart contracts and/or encryption, blockchain technology, should allow the work of verifying credentials and the provision of access to verified credentials to take place in almost real-time.

It allows higher education institutions, employers, and others to verify credentials without manual processes, while simultaneously verifying the trustworthiness of credentials in real-time. There has been a noticeable increase in trust, a decrease in administrative burden, and less opportunity for fraud. Furthermore, the use of blockchain technology in credential verification has implications that go beyond education. A collective model for securely managing digital credentials could extend the use of blockchain technology to government documents, professional licenses, and certifications for medical assistance. Therefore, blockchain is a disruptive innovation and sets a new status quo of making a trustworthy, credible and fraud resistant verification service.

Among other areas of technology, verifying that processes are secure, transparent, and tamper-proof is now more important than ever in the context of certification, employment, and education. The process of certificates verification is time consuming and manual and also comes with the risk of loss, fraud, and forgery of information. Blockchain is a compelling technology to address some of these challenges due to the decentralization, unchangeable and transparent nature of blockchain.

The verification of professional and academic credentials is one of the issues that are of growing concern to governments, businesses, and educational authorities worldwide. Credential verification has primarily relied on either centralized databases or a paper-based process which are subject to being manipulated, fraudulent actions, inefficiencies, and large administrative costs. Such limitations are especially concerning in light of growing problems with forged diplomas, counterfeit degrees, and undocumented credentials.

2. Related work

For decades, document verification has been accomplished using manual processes and centralized databases systems. Signed documents are checked by authorized people and cross-checking signatures and seals are verified in the process of manual verification. Even though this is a simple method, it is long, requires a large number of human resources and is also likely to bear the influence of the human factor[1].

The centralized database systems are more modern approach where the organizations store the records in digital format of all provided licenses, certifications and identity documents. To confirm, the parties may request to inspect such documents. Although this is quicker than manual processes, centralized solutions also possess other disadvantages such as single point of failure, vulnerability to hackers as well as a high dependency on the authenticity of the central authority. The compromise of the central database may result in serious security vulnerabilities due to the alteration or destruction of all the related records[2].

A number of solutions have been developed using digital signatures, hash functions and watermarking as cryptographic algorithms to verify the values. The techniques increase the integrity and authenticity of documents as they incorporate distinct identifiers in the document. As an illustration, watermarking prevents a mere duplication, and the digital signature guarantees non-repudiation.[3].

Yet, such techniques frequently involve trusted certificate authorities or third party verification agencies, which involve extra costs and dependencies. Furthermore, if private keys are compromised or certificate authorities are attacked, the verification system becomes unreliable.[4]

Many organizations have moved towards cloud-based verification systems as a sector regarding cloud computing has progressed. These technologies minimize the necessity for physical verification through assured storing and retrieval of documents on secure servers. While the establishment and format of cloud platforms are user friendly and processes are more easily scalable, they are not completely safeguarded against data leaks, insider threats, or cyber threats and risks; in addition, further when you solidify it to a single service provider, it undermines decentralization and transparency as they have the power within their platform to remove/change/deactivate anything pertaining to your documents, therefore pulling the power into a singular entity outside of your control.[5]

In recent years, researchers, developers and practitioners have explored and exploited the utility of blockchain technology as a distributive form of document verification. Blockchain ensures that once a hash of a document is placed on a ledger, said hash can't be removed or modified without network consent. This lack of ability to tamper is what drives the immutability of documents within the platform of blockchain. [6]

Verification of University Certificates: Some universities had attempted to issue transcripts and degrees through blockchain networks. For example, MIT launched a blockchain-based format for digital diplomas that enable graduates to directly share their verifiable credentials with employers.[7]

Government Initiatives: Countries such as Estonia and India are experimenting with using blockchain for secure digital identities and land records as examples of the use of blockchain for language documentation. Commercial Platforms: Private companies are now developing blockchain-based verification systems to allow employers and recruiters to rapidly verify employment information.[8]

All multiple applications highlight the advantages of blockchains - they are decentralized, transparent, immutable and automate divisions using smart contracts. Overall, the articles reviewed provide evidence that blockchain has value as technology for secure, trusted verification of documents but they still need to be developed and validated for authenticating at scale.[9]

Beyond its current uses, blockchain-based verification of documents is being incorporated more and more with cutting-edge technologies like digital identity frameworks, zero-knowledge proofs, and the InterPlanetary File System (IPFS). By enabling decentralized document storage, IPFS lessens the need for centralized servers while guaranteeing successful retrieval. [10]

On the other hand, in zero-knowledge proofs, one side can prove that he or she has valid credentials without exposing the data used to generate the credential, maintaining privacy [11].

Similarly, with the integration with the standard of decentralized identity (DID), users can gain control over their credentials and share them only with the verifiers. Such developments will ensure that blockchain verification systems can be widely used in government, healthcare, education, and business ecosystems to improve security and privacy and also increase their reach to the global interoperability, cost-saving, and user-focusing control. [12].

Another research area is the legal and regulatory facet of blockchain-based verification. Blockchain ensures the immutability and decentralization, and its usage presupposes the international legal acknowledgment of the digital credentials. In recognition of digital identification and trust services, such as, countries in the European Union are establishing blockchain-based systems as per the eiders regulation. [13].

Nevertheless, the absence of standardized ones complicates the ability of different blockchain platforms to cooperate and leave credentials issued with the use of blockchain technology recognized by legal bodies. Consequently, international verification standards and the legal harmonization of the system are necessary in order to make the blockchain verification systems completely functional. [14].

The scalability, issues of cost effectiveness and access have to be addressed to allow widespread acceptance. The latency and transaction costs of the public blockchains, including Ethereum, limit their usability in large scale verification [15].

To overcome this and reduce the amount of computational overhead, researchers are exploring sidechains, permissioned blockchains, and consensus mechanisms such as Proof of Stake. Moreover, inclusivity is of the essence since the blockchain-based verification is not as available in most developing countries as they do not have the necessary infrastructure. Unless these problems of accessibility and performance are addressed, blockchain will not become a popular verification tool [16].

Another promising field of study is the integration of blockchain technology with artificial intelligence (AI) in order to detect intelligent fraud and verify. Blockchain ensures the precision and integrity of the records, whereas AI models can be trained to recognize abnormalities in the metadata of the documents, patterns of use, or suspicious verification requests. With the integration of the two technologies, one is able to identify the fraudulent activities in real time before they have propagated throughout the network which offers a proactive verification method [17].

There is also increasing interoperability of heterogeneous systems. Different blockchain frameworks, including Hyperledger Fabric, Ethereum, and Corda, are common with educational establishments, government agencies, and commercial enterprises. With lack of interoperability, organizations find it hard to exchange verified credentials. [18].

Also of significance to a socio-technical perspective are user trust and acceptance. Whereas blockchain has ensured immutability, end users (students, workers, or citizens) may be unwilling to accept blockchain-based credentials unless there are clear benefits, usability, and legal assurances. Thus, to encourage adoption, it is essential to use awareness campaigns, user-friendly interfaces, and open governance frameworks. Implementation of blockchain in verification is a social just as much as a technical challenge, research has determined [19].

The last sign of the future of blockchain in document verification is the development of decentralized ecosystems based on the combination of blockchain with the latest technologies such as edge computing, the Internet of Things, and digital identity frameworks. Indicatively, edge computing would ensure faster processing capability at the local nodes, and IoT-enabled devices may automatically create logs (in blockchain) of events (like healthcare tests, supply chain documents). A truly trust less, worldwide verification infrastructure could be established by these hybrid solutions, which would lessen dependency on centralized authorities and extend blockchain verification outside of government and education into a variety of industries including healthcare, supply chains, and legal services [20].

3. Proposed System

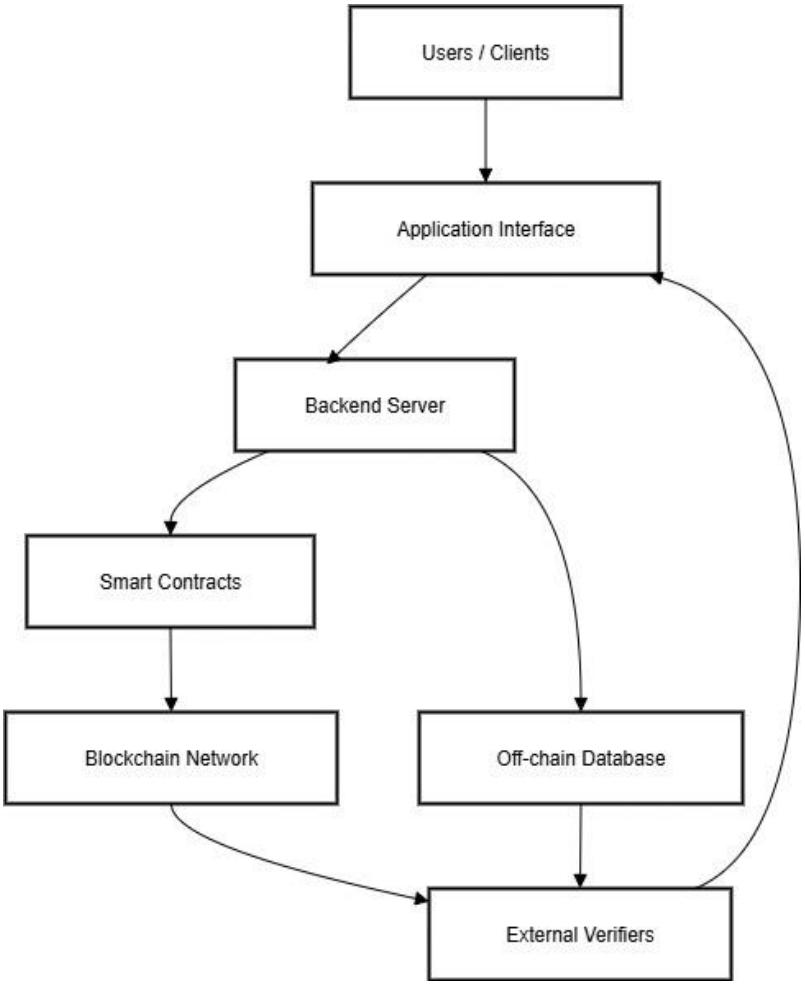
The proposed approach employs blockchain technology to establish a secure, transparent, and secure verification platform for documents. Unlike traditional document-verified documents, which are usually under centralized control or in some instances not verified manual, the system with records of

verification online on a decentralized ledger would ensure availability, legitimacy, and trust of the documents.

To avoid concerns of data overload and avoid privacy vulnerabilities in the suggested structure, documents are not stored directly on the blockchain. Instead, the records are produced as cryptographic hash values and stored on the chain. The hash values act as a pair of unique digital fingerprints for each document. Any alterations or falsifications made to the of documentation would produce a different hash, thereby flagging that the document has been altered.

The verification system provides the following key elements.

Along with secure key management and governance procedures, the system incorporates digital identities (DIDs) and role-based access for issuers, verifiers, and auditors.



The following elements are introduced by the system:

1.User Module

This module enables people, workers, or students to upload their documents for validation. The document is stored on the blockchain when the system creates a unique hash of it.

2. Authority Module

Credentials are created and sanctioned by official entities (government agencies, businesses and universities). They would verify the document by attesting to its authenticity via electronic signature via the document's metadata before sending the document to the blockchain.

3. Verification Module

A user (either an employer/recruiter, or other user) can verify the document. The user would upload the document to the platform; the platform would re-compute the uploaded document, compute a hash, and compare that hash to the hash on the blockchain. If the hashes match, the document is verified valid.

4. Blockchain layer

Allows the auditable, decentralized, immutable record keeping. The blockchain records the transaction including document registration, verification requests, and approvals, to guard against tampering and unauthorized changes.

5. Smart Contracts

Are capable of automating both the issuance and verification of documents. Their true value is in guaranteeing that verification requests are processed automatically, and will only be registered by parties that have been authorized to register documents.

Benefits of Proposed Systems:

1. You eliminate forgeries and fraud of documents and certificates.

2. You eliminate reliance on outside verification organizations.

3. You have a tamper-proof verification process that registers the verification in real-time.

4. You create an efficient, transparent, trustworthy process for verification of documents.

5. You save time and costs in verification.

6. Assurance of Authenticity: All documents are cryptographically signed and anchored onto the blockchain to guarantee that only the original issuer can create accurate documents.

7. Assurance of Data Integrity: Signatures with immutable hashes deter forgeries and tampering by indicating any change, even a minor one, in a document immediately.

4. Methodology

A. Requirement Discussion

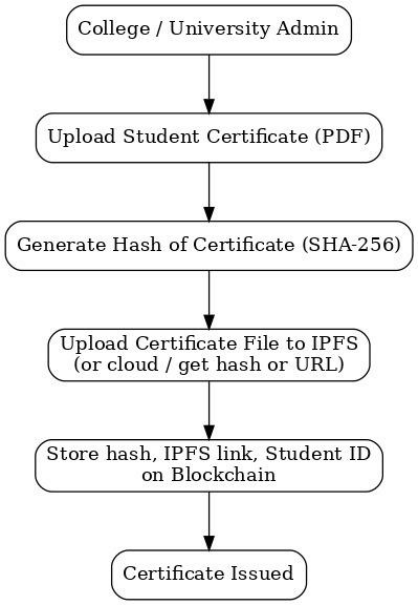
The first component in the stages is discussing requirements. Within this stage, some of the functional and non-functional requirements of the system are observed. Functional requirements would consist of capability to store document hashes on the blockchain with secure storage, perform real-time verification, smart contracts that automate the solution, and with role-based access for different stakeholders. Non-functional requirements include 'to be scalable', 'to be reliable', 'to be usable' and other functional aspects to assure this solution is functional and sustainable. More precisely establishing what the solution is attempting to achieve will drive the entire project from this stage.

B. System Blueprint

The process of designing the system will begin after the requirements have been reviewed. The system will be established into different modules, including a blockchain layer, off-chain storage, frontend, backend and supporting databases. Each module is designed to be compartmentalized and arranged to reduce integration between modules are developed so they model a system relying on each module. The blockchain is in place to assure the hashes of the stored documents have integrity and recorded in an immutable fashion, the frontend acts as the user interface, and the backend serves as an intermediary which handles request and function processes, while the databases and off-chain storage will handle various functions related to metadata and the original files while the smart contracts serve to create rules for access control and verification.

C. Development

This phase of iterative development involves the incremental development, evaluation, and improvement of modules. In development of the frontend, HTML, CSS, and JavaScript are leveraged to develop responsive and accessible applications. The backend uses the ASP.NET development framework to facilitate secure processing of user requests and connectivity to the blockchain network. As script hashing methods are developed, SHA 256 is emphasized for developing a unique identity for documents and the ability to quickly recognize if they have been tampered. With the incremental approach, some functionality is made available to be tested and to be enhanced as the whole.

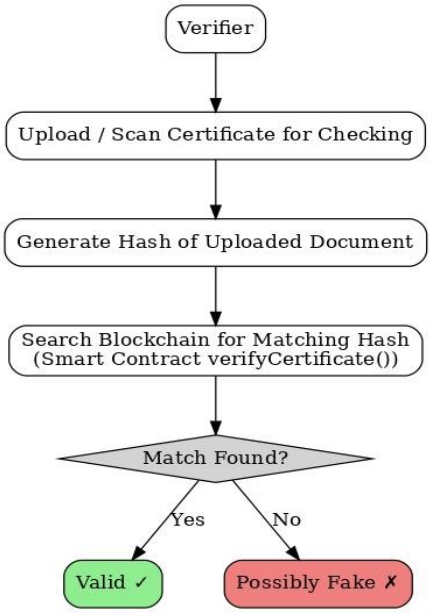


D. Validation and testing

After the development process, a thorough testing process is employed to the system. Unit testing is used to check specific modules and integration testing is used to verify that various parts of the system like the frontend, backend and blockchain work as expected. To ensure resistant to manipulation and unauthorized access, security testing is necessary to ensure it. Sample users are also subjected to user acceptance testing to make sure that the platform helps and is user-friendly. This extensive testing process will ensure the system is of quality standard prior to implementation.

E. Deployment and Maintenance.

The system will be stored in secure servers which have been provided with blockchain during the implementation process. The nodes of blockchain are configured to maintain a consensus and smart contracts are implemented to automate the verification. This is closely monitored to ensure that there is stability in the performance after deployment. Maintenance is the bug fixes, product enhancements, and updates of security measures. Future improvements can be made by adopting more advanced blockchain platforms, mobile apps support, and integration with national identity systems.



Technologies Used

A. The Blockchain Technology.

The basic system would be established based on blockchain technologies, which are immutable, decentralized and transparent instead of relying on a centralized database in which the record is stored in a single place: the record exists in the blockchain on nodes. The information stored in the blockchain should be governed by the same concepts of immutability. A shared trust of the documents is emphasized as the documents are each hashed and available within the blockchain and are only subject to change if a group consensus is enacted (by all parties involved in the hash).

B. The Smart Contracts.

Another underlying foundation of the system is leveraging Smart Contracts and their capability in validating documents. A smart contract is a self-executing application that logs attempts to validate access by issuer(s) and authenticate the document hash. Using automated verification to validate documents reduces the time it takes to validate a document from personal verification which can take some time and authenticate documents which may have required third-party authentication previously.

C. Cryptographic Hashing

A SHA-256 cryptographic hash is generated for each document; this will be a unique hash generated for each document. This is referred to cryptographic hashing which sign case is a fixed-length document. If the document is changed, it will create an entirely different hash; in turn, you will know that the

document has been changed or altered in any shape, form, or fashion. Also, it helps conserve space on the blockchain, we can store the document "off-chain," and store the hash "on-chain."

D. Frontend Technologies

HTML, CSS and JavaScript language is the technology used to develop the frontend for the system. These choose languages allow developers the ability to build an easy to use and responsive user-interface. The design is accessibility-friendly for both technical and non-technical users to upload and validate documents.

E. Back-end Technologies

ASP.NET is the back-end technology chosen for this system which helps the user-interface applications talk to and communicate with the backend database and blockchain that makes up the application. ASP.NET is secure, and enables scalability as well as it can easily communicate with MSSQL. The backend will authenticate all users and perform actions on behalf of the user, and send communication from the user-interface to the smart contracts.

Off-chain Storage and Database

Verification logs, user information, and metadata are all managed with MSSQL. Original papers are safely kept on off-chain storage, like cloud servers or institutional databases, because blockchain is ineffective at holding huge files. Scalability and privacy are both offered by this combination.

Security Frameworks

Security Frameworks Although authentication processes are used to ensure that the issuers are authorized, encryption security assists in ensuring that data flows between system components are secure to support secure operations. By offering non-repudiation, which makes it impossible for issuers to subsequently contest the legitimacy of the documents they provide, digital signatures increase trust.

5. RESULT AND DESCUSSION

The document verification system, based upon blockchain technology, has been developed and tested in order to explore and assess the capabilities of the system and to assess its remedies of the issues limiting document verification today. In summary, it was found that the system did meet some of its main objectives to which it was designed for, such as to mitigate document fraud, to verify documents as authentic, and to apply blockchain technology using fast and transparent verification methods.

During the testing period of the system, a variety of document types were enrolled in the platform; these included educational qualifications, identification and verification of identification, and a variety of

institutional records were held on the platform. Each document was hashed using a cryptographic method and the cryptographic hash was held on the blockchain. Each of the documents went through a verification process beginning with the original document and following with the modified document. As appropriate, there were modifications made to the document and when respect to the modification and verification, the system confirmed the document integrity based upon the original hash stored in the blockchain. For each document participants were able to confirm the validity of the document through the blockchain record confirming whether the document was valid or invalid.

A major finding of this project was the reduction in verification times. While verification can sometimes take hours or even days to complete depending on the institution and type of intermediaries, blockchain verification can be completed in seconds. Once we were able to compare the hash of the document to the blockchain record, verification was instantaneous, and this was an obvious time savings. This seems to support use cases where quick decisions are needed such as: hiring and student admissions; as well as, determinations in the area of justice.

Another major finding of this project was transparency and trust. The blockchain had the complete audit trail of all attempts to verify the document and all entries of the document's hash. Institutions and verifiers can see the history of validation of a specific document, without three-party verification. The audits and transparency created a sense of trust for users, and a lower chance of disputes about authenticity. The decentralized nature of the blockchain architecture was also a very important finding. This implied that there was no single authority that would alter or manipulate records and therefore there was no single point of failure.

They were also tested on the accessibility and usability of the system. The user interface that was developed using HTML, CSS, and JavaScript was found to be easy to navigate and user-friendly. Even the non-technical persons could find it easy to upload and validate the documents. Based on the feedbacks of the test users, the system was easy to operate and had comprehensive guidelines on each task. The integration of role-based access control also was efficient as it did not allow the unauthorized user to upload or alter data and still offered the verifiers an opportunity to download the document to verify it.

The security performance was achieved in regard to the objective of the project which was to prevent forgeries and unauthorized changes. The solution was also authentic and preserved privacy of the user by storing hash values of original documents and not the paper in the blockchain. Due to the automation of the verification procedure and strict rules that did not require human intervention, smart contracts became a necessity. Consequently, the probability of human error was reduced, as well as reliance on external parties.

The proposed solution proved to have several benefits in comparison to existing solutions, including manual verification or databases. Manipulation of data, insider threats and hacking are typical centralized systems issues. Conversely, the blockchain ledger proved to be far more reliable since it was

undamageable and could not be manipulated. Also, there was no need of external bodies or intermediaries to be involved, and thus the verification cost was reduced. The system is cost effective and hence attractive to its wide usage across the government agencies, businesses, and even across the universities.

Despite these optimal outcomes, the project, however, revealed some challenges and limitations. Scalability is still an issue since managing a very high number of documents might cause latency and higher transaction costs on public blockchains. Off-chain storage reduced blockchain load, but more modification was needed for connection with institutional systems that were already in place. Because blockchain-based systems depend on distributed networks to function, another drawback was their reliance on network connectivity. These difficulties point to areas that need additional investigation and improvement, such implementing hybrid solutions or using blockchain platforms that are more scalable.

Overall, the findings demonstrate that the suggested method accomplishes its goals and offers a safe, open, and effective framework for document verification. The results discussion emphasizes its benefits over conventional techniques, its high accuracy in detecting tampering, its potential to shorten verification times, and its effectiveness in fostering user trust. However, the constraints that have been discovered also open the door for future enhancements, guaranteeing that the system can develop into a more complete and broadly applicable solution.

6. Conclusion and Future Enhancement

By guaranteeing authenticity, transparency, and tamper-proof validation, the Blockchain-Based Document Verification System effectively overcomes the drawbacks of conventional verification techniques. The technology protects data privacy while enabling secure and real-time verification through the use of blockchain, smart contracts, and cryptographic hashing. It drastically cuts down on the amount of time needed for verification, lessens the need for middlemen, and increases user confidence through immutability and transparency.

In the future, the system can be enhanced with features like mobile application support, integration with national identity systems, and interoperability with institutional databases. Scalability can be improved by adopting advanced blockchain platforms or hybrid models. Additional technologies such as AI for fraud detection, biometric authentication, and compliance with global standards can further increase its effectiveness and broaden its applications across sectors like healthcare, property, and governance.

Reference:

1. J. A. Berrios Moya, J. Ayoade, and M. A. Uddin, “A Zero-Knowledge Proof-Enabled Blockchain-Based Academic Record Verification System,” Sensors, vol. 25, no. 11, p. 3450, 2025.

2. S. Begum, M. Priya, G. Swapnil, and G. S. Rani, “Blockchain Solution for Document Integrity and Forgery Mitigation,” International Journal for Research in Applied Science and Engineering Technology (IJRASET), vol. 13, no. 3, pp. 174–181, 2025.
3. P. M. Pondkule, R. Sharma, and A. K. Singh, “Implementation of Blockchain-Based Document Management System for Higher Education Organizations,” International Journal on Smart Sensing and Intelligent Systems, vol. 18, no. 1, pp. 1–12, 2025.
4. E. Maksina, V. Shmakov, N. Voinov, T. Leontyeva, and Y. Yusupov, “Implementation of a Blockchain-Based Software Tool to Verify the Authenticity of Paper Documents,” in Information Technologies and Intelligent Decision-Making Systems, Springer, 2024, pp. 71–83.
5. C. Antony, P. S. Shetty, V. Kumar, and S. S. Shetty, “Counterfeit Detection of Documents using Blockchain,” International Journal of Engineering Research & Technology (IJERT), vol. 13, no. 6, pp. 1–5, 2024.
6. D. Chiș and M. Caramihai, “Blockchain in Higher Education: A Secure Traceability Architecture for Degree Verification,” in Blockchain in Education, IntechOpen, 2023, pp. 101–120.
7. M. Aldwairi, M. Badra, and R. Borghol, “DocCert: Nostrification, Document Verification and Authenticity Blockchain Solution,” arXiv preprint arXiv:2310.09136, 2023.
8. M. R. Kumar, A. K. Singh, and P. R. Sinha, “Blockchain-Based Secure Certificate Verification System Using IPFS and Smart Contracts,” International Journal of Advanced Computer Science and Applications (IJACSA), vol. 15, no. 4, pp. 220–227, 2024.
9. F. Almarzouqi, S. Ellatif, and H. Al-Khazraji, “Blockchain for Digital Identity and Document Authentication in Government Services,” IEEE Access, vol. 12, pp. 45560–45572, 2024.
10. Y. Zhang, L. Chen, and H. Wang, “Blockchain-Based Document Timestamping and Integrity Verification for Legal Applications,” Future Internet, vol. 15, no. 9, p. 275, 2023.
11. T. Rahman, S. I. Mouno, A. Mojumder, A. K. Al Azad, and N. Mansoor, “Verifi-Chain: A Credentials Verifier using Blockchain and IPFS,” arXiv preprint arXiv:2307.05797, 2023.
12. B. Awaji and E. Solaiman, “Design, Implementation, and Evaluation of Blockchain-Based Trusted Achievement Record System for Students in Higher Education,” arXiv preprint arXiv:2204.12547, 2022.
13. “Secure document verification using blockchain and IPFS with …” (AIP Publishing), addressing security vulnerabilities and proposing a secure scheme.
14. Dr. S. Prabakaran, Dr.P.Anbumani , Muthuvel.S, Logesh Kumar.P, Ajithkumar.A, Ganeshprabhu.S, Fake News Detection Using AI.. Advances in Consumer Research. 2025;2(6): 2369-2374
15. “DIAR: a blockchain-based system for generation and verification of …” (Springer, 2024) – a system with generation, verification, and revocation features.
16. S. H. Said, M. A. Dida, E. M. Kosia, and R. S. Sinde, “A Blockchain-based Conceptual Model to Address Educational Certificate Verification Challenges in Tanzania,” Engineering, Technology & Applied Science Research, vol. 13, no. 5, pp. 11691–11704, 2023