IJARSCT

International Journal of Advanced Research in Science, Communication and Technology

International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal

ISSN: 2581-9429

Volume 5, Issue 10, May 2025

Impact Factor: 7.67

The Blockchain Based Document Verification System

Pushkar Chaudhari, Chaitanya Warade, Rushikesh Raut, Prof W. P. Rahane
Department of Information Technology Engineering
NBN Sinhgad Technical Institutes Campus, Pune, India

Abstract: *Document verification is a regular need for both individuals and corporations. Verifying the legitimacy of records is essential for anything from legal documents to academic degrees. In order to safely store and validate certifications, this study suggests a blockchain-based solution called "BlockDoc," which is primarily intended for use in educational institutions. The suggested method makes use of blockchain technology and cryptographic hashing to guarantee the validity and integrity of documents. The framework transforms document content into a one-way hash that is stored on the blockchain using cryptography. Each document is uniquely identified by its hash, facilitating easy and safe verification. A document is considered legitimate if its hash matches the hash stored on the blockchain. This technology improves the effectiveness of document verification procedures and removes the possibility of tampering.*

Keywords: blockchain; cryptographic; hash code; certificates; Ethereum..

I. INTRODUCTION

A blockchain is a distributed, decentralized digital ledger made up of an ever-expanding list of items known as blocks that are safely connected by means of cryptographic methods. A block cannot be changed or withdrawn from the blockchain after it has been added without rendering the entire chain invalid. Blockchain is a transparent and safe way to store and transfer data without the need for middlemen because of its immutability and tamper-evident nature.

Blockchain technology has potential uses in a wide range of sectors, including supply chain management, healthcare, education, and finance. Blockchain provides a novel way to counteract the growing number of fraudulent documents and certificates in the context of document verification. It takes a lot of time and resources to confirm the legitimacy of the many diplomas that educational institutions, in particular, issue each year.

Blockchain technology is used by the "BlockDoc" system to safely store and validate educational credentials. The solution removes the possibility of tampering and guarantees data integrity by transforming document content into cryptographic hashes and storing them on a blockchain. The creation and deployment of the "BlockDoc" system are described in this paper, demonstrating how it has the potential to completely transform document verification procedures.. This can ameliorate translucency, security, and effectiveness. The verification system mentioned can also be an important aspect of DApp. By having a way to corroborate the authenticity of the diploma, one can ensure that it has not been tampered with or altered in any way[6]. It is also important to have a training system in place to help ameliorate the delicacy of the verification system. By continually repeating and perfecting the system, one can make it more dependable and effective over time. With the growing interest in decentralized systems, DApp could have significant eventuality for relinquishment and growth..

II. LITERATURE SURVEY

One of the affects that job suppliers frequently perform is the most popular method of demonstrating the legitimacy of warrants. It takes a lot of time for work suppliers to provide interview findings; therefore, a genuineness verification procedure tool is needed [7]. Organizations typically do verification for a considerable amount of time. They create a blockchain-based warrant confirmation method to address this problem. Issues arise while verifying the validity of the instruments, which often takes up the majority of the day, and there is a chance for fake instruments. Scholastic instruments provided by tertiary institutions really use written versions to be sent to researchers. False warrants have been issued numerous times. One of the issues they tackle is the reduction of counterfeit instruments through blockchain innovation [9], as the blockchain has the ability to record instrument data.

The created computerized hand is also placed on the device and is used to verify the existence of the material archives using the sophisticated hand on the device. The study by Triand et al. [10] introduces computerized report security on sanctions high level training warrants with advanced hand and sha1 calculation. The system makes use of the Ropsten network's public blockchain. A computerized confirmation method in the field of lemon training is presented by creating an Ethereum blockchain-grounded report check clever contract for the Moodle proficiency 1 activity system[11] using a brilliant agreement grounded system that is connected to the Moodle education system[12] model.

However, the system built does not use blockchain innovation. Actual report affirmation with perceptual hash[13] illustrates the process of electronic affirmation on the requirement that actual records be completed electronically. This issue demonstrates that actual archives will have different hash esteems each time they are digitized, and the results get to show how affirmation with a hash can both uncover that the electronic train has been changed and uncover the first train.

They suggested the 2048-piece RSA computation, the AES 256-cycle, and the sha 256 for computerized signatures and encryption. Advanced hand execution of AES 256-bit and RSA 2048-cycle for safe. The lack of tools for the increasing number of material extortion cases [15] has led to the proposal of blockchain innovation as a solution. One element of the suggested approach that would address the problem is the placement of all unique IDs on the blockchain. Every year, understudy scales are conducted by several colleges. Every graduate will possess a degree and a warrant. One can use warrants to pursue jobs or more training. Through hash code verification or QR scanning, the literature review describes the different systems. The user will only be able to choose from one choice, though. Both choices are available to the user in the proposed system, and the user is free to choose among them.

III. PROPOSED SYSTEM

The "BlockDoc" solution combines cutting-edge cryptographic methods with blockchain technology to guarantee safe document verification and storage. Forgery, inefficiency, and dependence on middlemen are some of the issues with conventional document verification procedures that the system is intended to solve. The suggested framework provides a strong and transparent solution for educational institutions and other organizations by utilizing the decentralized and unchangeable feature of blockchain technology.

System Architecture

Three fundamental components make the foundation of the "BlockDoc" system's architecture. Document Owner (Prover): Uploading documents to the system is the responsibility of the Document Owner (Prover). Before putting their papers on the blockchain, the document owner creates unique hashes for them using cryptographic techniques.

Verifier: The organization that makes the request for document validation is the verifier. To ascertain validity, they use the system to compare the hash of the supplied document with the hash kept on the blockchain.

Blockchain Network: The blockchain network stores document hashes in a decentralized ledger. It guarantees the transparency and immutability of data saved, offering a certificate of document validity that cannot be altered.

Workflow

The following steps are part of the "BlockDoc" system's workflow:

Generation of Hashes:

The system creates a distinct digital fingerprint for each submitted document using a safe hashing method (SHA-256, for example). The original text is secure since this hash is a one-way function that cannot be undone.

Blockchain and IPFS storage:

A smart contract on the Ethereum blockchain stores the created hash, establishing an unchangeable record of the document's integrity. The InterPlanetary File System (IPFS), a decentralized storage network that lessens the data burden on the blockchain, is where the document is kept.

Procedure for Verification:

A verifier submits the document to the system upon requesting validation. The submitted document's hash is recalculated by the system, which then compares it to the blockchain's hash. The document is considered legitimate if the two hashes match.

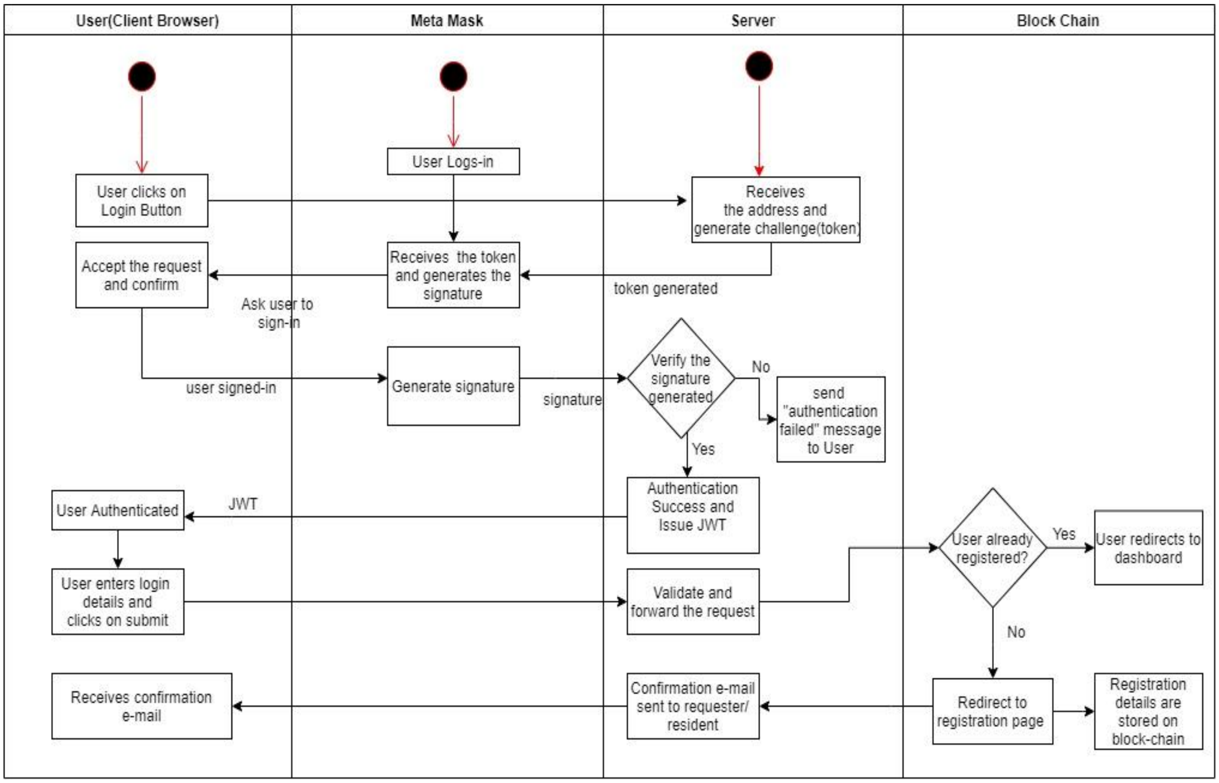
User(Client Browser)
Meta Mask
Server
Block Chain
User Logs-in
User clicks on Login Button
Receives the address and generate challenge(token)
Accept the request and confirm
Receives the token and generates the signature
token generated
Ask user to sign-in
user signed-in
Generate signature
signature
Verify the signature generated
No
send "authentication failed" message to User
Yes
User Authenticated
JWT
Authentication Success and Issue JWT
User already registered?
Yes
User redirects to dashboard
User enters login details and clicks on submit
Validate and forward the request
No
Receives confirmation e-mail
Confirmation e-mail sent to requester/ resident
Redirect to registration page
Registration details are stored on block-chain

Fig. 1. Example of work flow of system

The purpose of this research is to create a website model for verification and validation of blockchain-based e-certificate data using QR codes that can prove the e-certificates received by webinar participants to avoid falsification of digital assets in order to follow the acceleration of digital transformation. This website architecture can also later be used as proof of the validity of the e-certificate obtained from the webinar organizer, so that if the digital signature in the e-certificate is correctly issued by the organizer then the display of encryption will be displayed on behalf of the participant's name in the verified e-certificate.

Verification of web-based Blockchain-based e-Certificate Validation is carried out in 4 research stages, including requirement identification, planning, design of prototypes/architectures, and the last stage of prototype review that has been designed that can be seen in the image below:

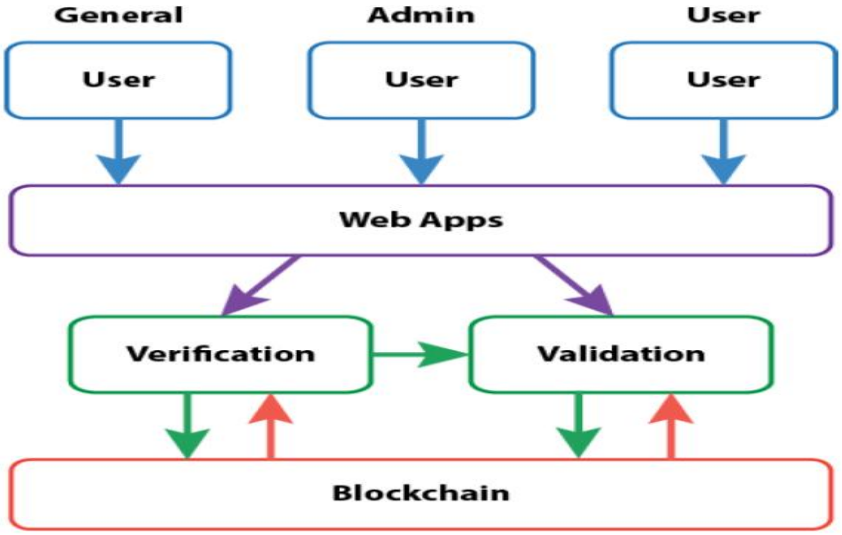

Fig. 1. Basic Blocks of the system

The BlockDoc system's development methodology is divided into five main stages, guaranteeing a methodical approach to building a safe and effective blockchain-based document verification system. The following is a breakdown of these phases: System design and requirement analysis: A comprehensive requirement analysis and architectural design form the system's cornerstone. System requirements are established during this stage, with an emphasis on essential elements like:

User Roles: To provide transparent operation and security, separate roles should be defined for administrators, document uploaders, and verifiers. hashes against the blockchain to confirm authenticity. Creating intuitive user interfaces for uploading documents and entering metadata is known as upload interface design.

Verification Endpoints: Setting up systems to enable verification for the validity of documents. Because of its integration capabilities, security, and scalability, the blockchain technology was carefully selected. Ethereum was chosen because of its strong smart contract capabilities, and document metadata is stored decentralized via IPFS (Interplanetary File System).

Integration with Blockchain To provide improved security and data immutability, the system incorporates blockchain technology. Smart contracts on the Ethereum blockchain are used to record document hashes, making it possible to identify any illegal changes or tampering.The foundation for automating tasks like storing, retrieving, and validating document hashes is provided by smart contracts.

IPFS Storage: By avoiding the drawbacks of keeping big documents directly on the blockchain, decentralized storage guarantees scalability.

Mechanism for Uploading and Hashing Documents:

This stage entails putting cryptographic methods into practice to provide a safe and impenetrable representation of every document:

Document Hashing: Each document is given a distinct digital fingerprint created by the SHA-256 hashing algorithm. This guarantees that even a small change to the text will produce a hash value that is entirely different.

Upload Mechanism: Documents and related information may be uploaded by users using an easy-to-use interface. The document itself is saved on IPFS, while the hash and metadata are safely kept on the blockchain.

Verification of Documents :To verify the validity of documents, the system offers a strong verification mechanism:

Verification Module: Verifies authenticity and integrity by comparing the uploaded document's hash with the hash recorded on the blockchain.

Document Retrieval: To enable transparent and trustworthy validation, the system gets pertinent data and metadata from the blockchain. This guarantees a clear and effective end-to-end procedure for confirming the authenticity of papers.

Deployment, Optimization, and Testing
During a crucial stage of the development process, thorough testing and optimization are required:
System Testing: To find and fix any problems, functional, security, and performance tests are carried out.
Optimization: To guarantee speedy document verification, lower latency, and smooth scaling, performance enhancements are put into place.
Deployment: To guarantee dependability and credibility, the completed system is put into use while abiding by security and legal requirements.

IV. IMPLEMENTATION

A block is a part of the blockchain in which it records all the transactions and once it is completed enters into a permanent database in the blockchain. In Blockchain, the blocks are linked one after other like a linked list. Every block consists the hash of the previous block as shown in Figure

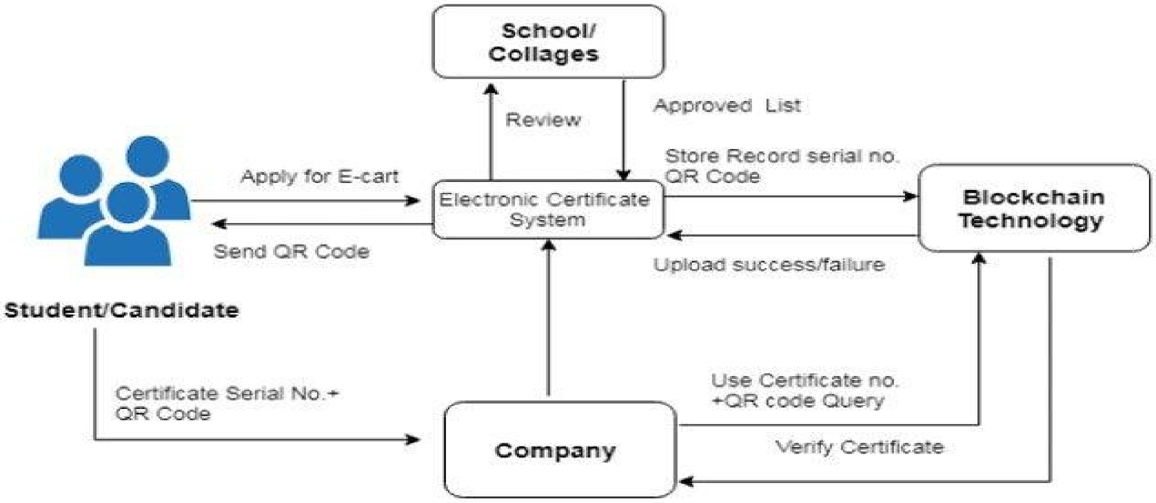

Fig. 2. Working architecture of the system

Blockchain consists of a set of nodes formed like a peer to peer network. With the help of public/private keys, users can interact in the blockchain. The private key is used to sign their own transaction and is addressed in the network with the public key. It provides authentication, integrity, and non-repudiation in the network.
Each node in the blockchain makes sure that incoming transaction is valid before transmitting further. Invalid transactions are discarded. [3] Each Blockchain network should provide certain rules for each database transaction. These rules are programmed to each blockchain client, then verifying that incoming transaction is valid or not. [7]
Database
A key defining aspect of any database-dependent application is its database structure. The database design can vary depending on many different factors, such as the number of reads over writes or the values that the user is likely to request the most. That is because as full stack developers we want the database to have the best performance.
Math Model
The mathematical model underlying a blockchain-based document verification system is essential for ensuring security and integrity. Cryptographic algorithms play a crucial role in this model, providing the foundation for hashing and

encrypting data. For example, secure hashing algorithms like SHA-256 generate unique digital signatures for documents, allowing any changes to the document to be immediately detectable.

Model Selection and Training:
The engine for the Blockchain-Based Document Verification System is designed to ensure the authenticity of research papers by using blockchain technology. The system analyzes various document attributes like metadata, content hashes, authorship, and submission dates. Through this model, documents are hashed using cryptographic techniques (e.g., SHA-256), ensuring the integrity of each paper. The blockchain stores these hashes to guarantee that the document has not been altered after submission. By leveraging a decentralized ledger, the system provides transparent and reliable verification of academic papers.

Model Evaluation and Optimization:
The module uses cryptographic techniques and smart contracts to evaluate document authenticity. The blockchain acts as a permanent and immutable record for each paper, storing document hashes and metadata. This module provides an interface for users to submit papers, verify their authenticity, and track their history. The system optimizes verification processes by ensuring high-speed access to data and minimizing transaction costs on the blockchain. Interactive visualizations help users understand the verification process and the data influencing each document's authenticity. Multilingual support ensures that researchers and institutions worldwide can access and use the system.

Deployment
For document verification, the system deploys on a public or private blockchain (such as Ethereum or Hyperledger) depending on user requirements. The use of cryptographic hash functions ensures that documents remain tamper-proof. With the blockchain's decentralized nature, each document is linked to its respective metadata in a transparent and immutable manner. The system’s performance is validated by its ability to verify documents quickly while ensuring accuracy and minimizing transaction fees. Once deployed, the system provides a robust and scalable solution for academic institutions to check document authenticity.
Cryptographic Evaluation: Uses information and hashes recorded on the blockchain to verify the validity of documents.
Optimization: Guarantees minimum verification delays, low transaction costs, and quick data access.

V. BENEFITS

Increased Document Authenticity: The system helps ensure the authenticity of research papers by verifying document integrity using blockchain technology. This prevents the submission of altered or plagiarized research, enhancing academic credibility and trust.
Cost-Effectiveness: By decentralizing the verification process, the system reduces reliance on manual checks, which can be time-consuming and resource-intensive. Academic institutions and researchers benefit from lower administrative costs and faster verification times.
Transparency and Security: The use of blockchain provides an immutable, transparent record of document submissions. Every transaction is securely recorded, making it impossible to alter a document after submission without detection. This increases trust among academics, researchers, and institutions.
Market Viability (Academic Credibility): By offering a reliable document verification system, academic institutions, publishers, and researchers benefit from greater credibility. The system ensures that only verified, authentic research is shared or published, which improves the reputation and reliability of academic outputs.

VI. FUTURE SCOPE

Incorporating Advanced Cryptographic Techniques:

The system can incorporate advanced cryptographic techniques such as zero-knowledge proofs to further improve security and privacy while verifying documents. This could enhance the user experience by providing verification without revealing sensitive document details.

Expanding Use Cases:

The system can expand to include different document types (e.g., patents, contracts, and certificates) beyond academic papers. This would make the blockchain-based verification system a more versatile tool across industries, from legal to healthcare.

Global Applicability:

Adapting the system to support international academic standards and languages can improve its global applicability. By integrating region-specific regulations and multilingual support, the system could be used universally by researchers and institutions worldwide.

Mobile Integration:

A mobile application for the blockchain-based document verification system could enable on-the-go verification for researchers, academic professionals, and institutions. With mobile access, users can quickly check the authenticity of research papers from any location, improving efficiency and accessibility.

Real-Time Updates and Smart Contract Automation:

Integration with smart contracts to automate document submission and verification processes can enhance system efficiency. The system could include real-time notifications and updates about document status, making the process faster and more transparent.

Interoperability with Other Verification Systems:

The future scope includes interoperability with other existing document management or verification systems (such as plagiarism detection tools) to provide a more holistic document validation process.

VII. CONCLUSION

The system can descry the credibility of electronic records warrants and emphases with train-grounded Ethereum blockchain innovation, so the train-grounded confirmation cycle can assist with faking warrants and emphases and make check simpler, with the train supplanting distributed exhibitions of warrants and emphases so that it'll be more opportune in spending paper, the consequences of testing the deal time from train to Ethereum is 1 second from each endlessly train honesty demonstrates assuming the train is harmed, changed, or the hashed will be not quite the same as the first on the Ethereum blockchain, so the train is distinguished for validness on Ethereum blockchain is a train that has not been changed and distorted, and hashes from the first train put away on an Ethereum.

Utilizing a system grounded on blockchain innovation can diminish the distortion of electronic records, in light of the fact that the most common way of distributing and check is done straightforwardly inside the system, the system can ensure the data gave is right with the right delicacy.

VIII. ACKNOWLEDGMENT

We would like to express our sincere gratitude to all those who contributed to the successful completion of our final year project, Blockchain-Based Document Verification System (BlockDoc). First and foremost, we are thankful to our project guide, Prof W. P. Rahane sir, for their continuous support, expert guidance, and valuable suggestions throughout the development of this project.

We also express our gratitude to the Department of Information Technology, NBN Sinhgad Technical Institutes Campus (NBNSTIC), for providing the required resources, infrastructure, and an encouraging research environment.

We would like to thank our Head of Department and the faculty members for their consistent support and insightful feedback, which helped us stay on track and refine our approach.

We acknowledge the open-source developer communities behind tools and technologies such as Ethereum, IPFS, Web3.js, Node.js, and MongoDB, which were essential to building this decentralized platform.

We also extend our appreciation to our peers, family, and friends for their encouragement and motivation throughout this journey..

REFERENCES

[1]. Husain, “Printed Document Integrity Verification Using Barcode,” JurnalTeknologi (Sciences & Engineering), vol. 70:1, p. 99–106, 2014.

[2]. Thuraisingham, “Blockchain Technologies and Their Applications in Data Science andCyber Security,” in 2020 3rd International Conference on Smart BlockChain (SmartBlock),Texas, 2020.

[3]. J. Jayachitra, Dr. S. Matilda, A. Gayathiri, “Certificate validation using blockchain,” in 2020 7th International Conference on Smart Structures and Systems (ICSSS), Villupuram, 2020

[4]. Barbara Guidi, Andrea Michienzi, Laura Ricci, “Data Persistence in Decentralized Social Applications: The IPFS approach,” in 2021 IEEE 18th Annual Consumer Communications &Networking Conference (CCNC), Italy, 2021.

[5]. Emmanuel Nyaletey, Reza M. Parizi, Qi Zhang, Kim-Kwang Raymond Choo, “BlockIPFS -Blockchain-Enabled Interplanetary File System for Forensic and Trusted Data Traceability,” in 2019 IEEE International Conference on Blockchain (Blockchain), USA, 2019.

[6]. Alexander Von Tottleben, Cornelius Ihle, Moritz Schubotz, Bela Gipp, “Academic Storage Cluster,” in 2021 ACM/IEEE Joint Conference on Digital Libraries (JCDL), Germany, 2021.