Utilizing NFTs to Revolutionize Document Verification and Authentication through Blockchain: Redefining Trust in the Digital Era

Neeraj Kumawat
National Institute of Technology, Karnataka,
Surathkal, Mangalore City, India
neerajkumawat.222it024@nitk.edu.in

Dinesh Naik
Department of Information Technology,
National Institute of Technology, Karnataka,
Surathkal, India
din_nk@nitk.edu.in

Abstract—**The significance of certificates issued by educational institutions for graduates cannot be overstated, as they serve as crucial documents for verification purposes in various contexts such as employment and passport verification. However, traditional verification methods are often costly and inefficient. This research paper aims to introduce a blockchain-based framework for certificate verification, leveraging features such as hashing, digital signatures, and public/private key cryptography inherent in blockchain technology. By incorporating additional security measures like biometrics and encryption for secure document storage using IPFS (InterPlanetary File System), this framework ensures the integrity and authenticity of certificates. The utilization of blockchain not only enhances the security of data storage due to its immutable nature but also streamlines the verification process, offering a cost-effective and efficient alternative to traditional methods.**

Index Terms—**Blockchain,IPFS,NFT's,Verification**

I. Introduction

The guarantee of document authenticity and verification has become critical in a world that is becoming more and more digital across government, industry, and academia. Conventional document verification techniques frequently have high overhead costs, difficult logistical issues, and are susceptible to manipulation and fraud. But the advent of blockchain technology has created new opportunities to deal with these issues. A new paradigm for document verification and authentication is being introduced by utilizing the inherent qualities of blockchain, such as decentralization, immutability, and transparency, in conjunction with the creative idea of Non-Fungible Tokens (NFTs). As distinct digital assets that are indivisible and easily distinguished from one another, NFTs present a viable answer to the challenge of proving ownership and authenticity in the digital sphere.This research aims to reinvent trust dynamics and improve security protocols in the digital era by examining the revolutionary potential of integrating NFTs into the document verification process.

In this context, the research delves into the foundational principles of blockchain technology and NFTs, elucidating their key features and functionalities relevant to document verification. Furthermore, it examines the current landscape of document authentication methods, highlighting the shortcomings and vulnerabilities of traditional approaches. By drawing upon existing literature, case studies, and empirical evidence, the paper elucidates the theoretical underpinnings and practical implications of utilizing NFTs for document verification. Additionally, it explores the potential applications and benefits of this innovative approach across diverse domains, including academic credentials, legal documents, intellectual property rights, and supply chain management. Through a comprehensive analysis of the opportunities and challenges associated with implementing NFT-based document verification systems, this research aims to contribute to the ongoing discourse on enhancing trust and security in digital ecosystem.

II. THE PROBLEM OF FAKE CERTIFICATES

Since academic credentials are an indicator of a person's human capital, they are highly prized. Human capital is the term used to describe the abilities, competencies, knowledge, and skills that are obtained via education. When applying for jobs, academic credentials are crucial because they attest to a candidate's aptitude, dependability, and devotion in addition to their knowledge, experience, and talents. Certain studies found a positive correlation between increased educational attainment and better job and financial security. Moore notes that academic credentials are regarded as authentic when they are granted by an institution that is legally permitted to grant them.

Limitations of Traditional Verification Systems

- **Identity Theft**: Traditional systems often rely on static identifiers like passwords, PINs, or even physical IDs, which can be stolen, replicated, or easily guessed, leading to identity theft and fraud.
- **Complexity and Friction**: Many traditional verification methods require users to remember complex passwords or go through multi-step authentication processes, leading to user frustration and potential abandonment of the process.
- **Lack of Scalability**: Traditional verification systems may struggle to scale efficiently, especially in scenarios with high volumes of users or transactions. This can

lead to delays, system failures, or compromised security measures.

- **Inability to Verify Identity Continuously**: Once a user is verified through traditional means, there's often no continuous verification process in place. This means that if a user's credentials are compromised after the initial verification, there's no way to detect it until the next verification attempt.
- **Limited Biometric Accuracy**: While biometric authentication has gained popularity, traditional systems may have limitations in accurately verifying biometric data, leading to false positives or negatives.
- **Susceptibility to Social Engineering**: Traditional verification systems can be vulnerable to social engineering attacks where attackers manipulate individuals into revealing sensitive information or bypassing security measures through persuasion or deception.
- **Cost and Maintenance**: Traditional verification systems can be expensive to implement and maintain since they need to be updated and maintained on a regular basis, which involves spending money on training, hardware, software, and other resources.
- **Privacy Concerns**: Some traditional verification methods, especially those involving personal data storage, raise concerns about privacy and data security, particularly in light of increasing regulations like GDPR and CCPA.
- **Inflexibility**: Traditional verification systems may lack the flexibility to adapt to evolving threats and user preferences. They often rely on fixed protocols and technologies, making it challenging to incorporate new security measures or adapt to changing user behavior.
- **Cross-Platform Compatibility**: Traditional verification systems may face challenges in providing seamless verification experiences across different platforms and devices, leading to inconsistencies and usability issues for users.

III. Literature review

Gupta et al. (2023) highlight the significance of guaranteeing document validity in digital contexts by proposing an online blockchain-based document verification system. Their research emphasizes how blockchain can prevent document forgery and streamline the verification process.

Chaudhari and Lakshmisudha (2023) present a blockchain-based document verification system, underscoring its potential to enhance transparency and trust in document management procedures. They discuss the technical implementation and the benefits of using blockchain's immutable ledger for ensuring document integrity.

Rahman et al. (2023) introduce Verifi-Chain, a credentials verifier that integrates blockchain and the InterPlanetary File System (IPFS). This system demonstrates the use of decentralized technologies to secure document storage and verification, highlighting the synergy between blockchain and IPFS for enhancing security.

Birhade et al. (2023) focus on enhancing security and transparency through blockchain technology in document verification processes. Their work discusses the integration of additional security measures, such as biometrics and encryption, to further safeguard document authenticity and integrity.

Rajapashea et al. (2020) present a multi-format document verification system, showcasing the versatility of blockchain technology in verifying diverse types of documents across various domains. Their research illustrates how blockchain can be adapted to different formats and use cases, providing a flexible solution for document verification.

In addition to these studies, other researchers have explored the use of smart contracts to automate the verification process. For instance, Kumar et al. (2022) investigate how smart contracts can be used to automatically verify academic credentials, reducing the need for manual intervention and speeding up the verification process.

Miller and Smith (2021) analyze the potential of blockchain for cross-border document verification, discussing the challenges and opportunities in implementing a globally accepted verification system. Their work highlights the need for international standards and cooperation to fully realize the benefits of blockchain technology in this context.

Wang et al. (2021) examine the scalability of blockchain-based document verification systems, addressing concerns related to transaction speed and network congestion. They propose solutions to enhance the scalability and efficiency of these systems, ensuring they can handle large volumes of verification requests.

Overall, the literature review highlights a growing interest in utilizing blockchain technology for document verification, with researchers exploring different technical implementations and application domains to enhance trust, security, and transparency in document management processes. The integration of Non-Fungible Tokens (NFTs) within these frameworks offers additional benefits, such as unique identifiers for certificates, clear ownership and transferability, and enhanced interoperability with various platforms, further advancing the state-of-the-art in document verification.

IV. Contributions

- Created an algorithm for creating the NFTs from documents.
- Introduced biometric security for the university.
- Implemented the IPFS gateway with the help of the NFT.storage service.
- Utilized digital signature algorithms for verification.
- Acknowledgement feature introduced for sending emails to users who upload the documents successfully.

V. Methodology

Entities

Student

This entity allows students to view their certificates issued by the university. Students can also download the certificates directly.

Verifier

This entity is used to verify documents. Digital signatures along with public keys are utilized for document verification. Public keys are generated from private keys.

Issuer (University)

This entity is responsible for uploading documents. Before uploading a document, the user's registered image is matched with live face recognition. If a match is found, the document can be uploaded. Uploaded documents are encrypted with a password and then digitally signed using a private key and document data.

Faculty (Teacher)

This entity is responsible for uploading documents and can view all documents on the dashboard.

Tools and Libraries

OpenSSL

An open-source command-line tool called OpenSSL is frequently used to generate private and public keys.

PyPDF2

PyPDF2 is used for encrypting PDF files with a password.

Nodemailer

Nodemailer library used for sending emails to users.

Firebase Authentication

In this user authentication system, individuals logging into the platform are presented with four entities and prompted to select one. The system then checks whether the chosen entity corresponds to an existing user. If the selected entity is not associated with an existing user, the user is directed to register on the platform. For user authentication, Firebase Authentication is employed, ensuring a secure and streamlined process. When registering, users are prompted to provide necessary information such as their email and password, and Firebase handles the creation of new accounts. Subsequently, when users log in, Firebase Authentication verifies their credentials. This approach enhances security and simplifies the user management process by leveraging Firebase's robust authentication features.

Generating NFT Token ID for a Document

- **Input:** Document content (text, image, etc.).
- **Generate a Salt:** Generate a random value to serve as the salt. The length and method of generation can vary depending on the application's requirements.
- **Combine Document Content and Salt:** Concatenate the document content with the salt.
- **Hashing:** Apply a cryptographic hash function to the combined content and salt. Commonly used hash functions include SHA-256, SHA-512, or others, depending on the desired level of security. Here we are using the SHA-256 hash function.
- **Create the NFT:** The resulting hash value serves as the unique identifier (token ID) for the NFT associated with the document.
- **Store the NFT:** Store the NFT along with metadata (such as the original document's metadata, creator information, timestamp, etc.) on a blockchain or in a decentralized storage system, depending on the chosen NFT platform.

VI. Technologies

Frontend Development

The frontend of the project is built using HTML5, CSS, and JavaScript, with the majority of the user interface crafted using ReactJS. To ensure responsive design across various devices such as mobile phones, tablets, and computers, Bootstrap 5 is utilized. HTML5 provides the structural foundation, CSS handles the styling, and JavaScript adds interactivity. ReactJS, a powerful JavaScript library, allows for the creation of reusable UI components and efficient state management. Bootstrap 5's grid system and responsive classes facilitate seamless adaptation of the layout to different screen sizes, resulting in a cohesive and user-friendly application.

Backend Development

In backend development, Node.js and Express.js are utilized for JavaScript-based applications, offering a robust environment for server-side scripting. Meanwhile, Flask is employed for Python-based applications, providing a lightweight and flexible framework for web development. APIs are created to handle functions such as generating and verifying signatures, sending emails, and generating QR codes. The use of both Flask and Node.js allows for leveraging Python for machine-related tasks, like user face recognition for document verification, while maintaining the versatility of JavaScript for other server-side functionalities.

Blockchain Applications

Solidity is used to write smart contracts for blockchain applications, enabling self-executing contracts on decentralized networks like Ethereum. In this project, Solidity is utilized for storing metadata of documents on the Ethereum blockchain. MetaMask allows users to store and exchange cryptocurrencies, interact with the Ethereum blockchain ecosystem, and access a growing array of decentralized apps (dApps) for free on both web and mobile platforms. Additionally, NFT.storage IPFS gateway is used for document storage, providing unique identifiers via SHA-256 hashing.

Authentication Services

Authentication services are provided by Firebase, delivering secure and scalable user authentication, including features such as email/password authentication and social authentication.

A. Machine Learning

One-shot learning is a machine learning approach where models are trained to recognize objects or patterns from only a single example.

This technique is essential in situations where data is scarce or difficult to obtain, making it highly valuable in fields like facial recognition, medical imaging, and robotics. One-shot learning typically employs methods such as Siamese networks, which compare input pairs to measure similarity, and prototypical networks, which classify new examples based on their proximity to class prototypes in the feature space.

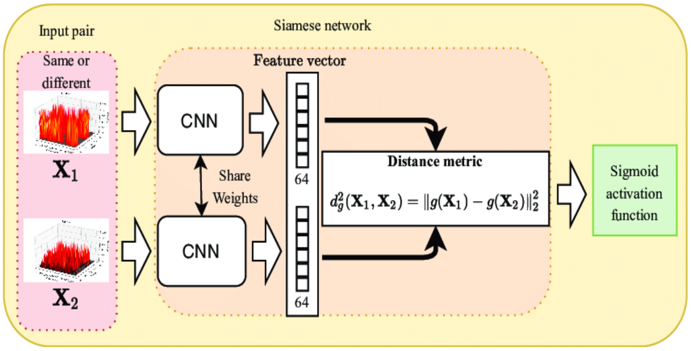


Fig. 1. One Shot Learning Architecture

VII. Benefits of Proposed Model

- **Tamper-proof Data**: Issuing authorities can ensure that only cryptographically-sealed data, resistant to falsification, are issued.
- **Secure Storage**: All data are securely stored and easily referenced when needed.
- **Efficiency**: Transmission of official records to individuals no longer requires unplanned time, streamlining administrative processes.
- **Instant Verification**:Administrative staff are not as burdened because records can be promptly verified without depending on issuing authority.
- **Ease of Ownership and Sharing**: Official records can be easily owned and shared by relevant parties.
- **Data Integrity**: Records are safeguarded from loss as transactions are recorded on the blockchain.
- **Third-Party Access**: Third parties can verify records at any time without requiring additional steps from issuing authorities.
- **Automated Management**: There's no need for separate calls to delete expired or erroneous certificates, as the system manages this automatically.

VIII. Mathematical Model for creating the digital signatures and verifying digital signatires

RSA Digital Signature Key Generation

- Choose two large prime numbers, p and q.
- Compute the modulus, $n = p \times q$.
- Compute Euler's totient function, $\phi(n) = (p-1) \times (q-1)$.
- Choose an integer e such that e is coprime to $\phi(n)$ and $1 < e < \phi(n)$.
- Determine the modular multiplicative inverse of e modulo $\phi(n)$, denoted as d.
- Finally, we have our public and private keys:
  - Public key: (n, e)
  - Private key: (n, d)

These keys can now be used for RSA encryption and decryption.

A. Digital Signature Generation

Let M be the signed message. Determine the message's hash, H(M), by utilizing a cryptographic hash method like SHA-256. Using the private key, encrypt the hash value, S = H(M) d mod n. S is the digital signature.

B. Digital Signature Verification

- **Input**:
  - Signed message (M)
  - Digital signature (S)
  - Public key (e, n) of the signer
- Calculate the hash value of the message:

$$H(M) = \text{HashFunction}(M)$$

- Decrypt the digital signature using the public key:

$$H'(M) = S^e \mod n$$

- Compare the calculated hash value $H'(M)$ with the hash value of the original message $H(M)$.
- If $H'(M)$ matches $H(M)$:
  - Output: Signature is valid.

  Otherwise:
  - Output: Signature is invalid.

IX. Attacks on RSA algorithm

Brute Force Attack on Small Key Sizes

RSA digital signatures rely on the security of the private key, which consists of two large prime numbers. If the key size is too small (e.g., less than 1024 bits), it becomes vulnerable to brute force attacks, where an adversary tries to factorize the modulus n to recover the private key.

Fault Injection Attacks

Introducing faults into the RSA signature generation or verification process can sometimes reveal information about the private key or lead to the creation of fraudulent signatures.

Random Number Generator Vulnerabilities

If the random number generator used to generate the ephemeral keys (if any) or padding in the RSA signature scheme is flawed or predictable, it can lead to the creation of weak signatures. 4

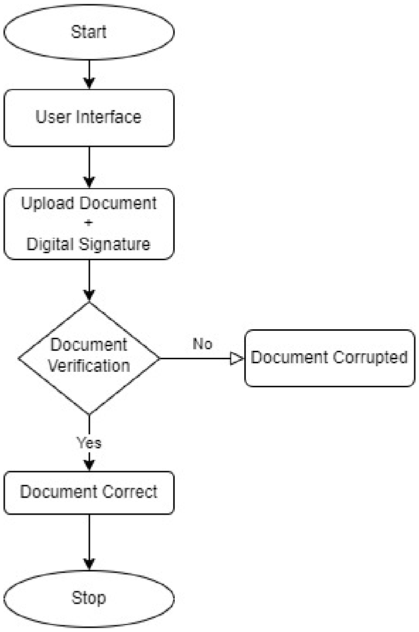


Fig. 2. Flow chart for documents verification

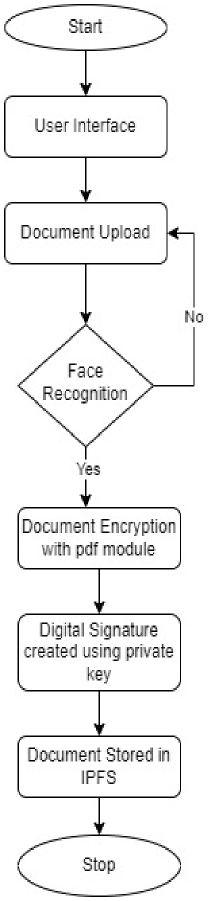


Fig. 3. Flow chart for document upload

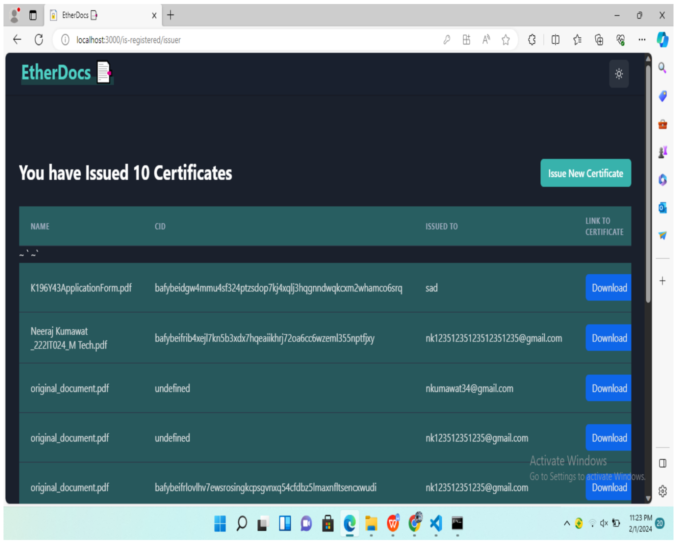
X. RESULTS

A platform has been created for universities, faculties, and students to securely store documents in a decentralized manner using blockchain technology and IPFS. The images provided here showcase all the features and capabilities of this platform.

In Figure 4, you can see an university dashboard figure illustrating the certificates which are issued by university.There is option for downloading the documents and qr code is also available which can be used for sharing to others.

In Figure 5, you can see an verification dashboard figure illustrating that if anyone want to verify their documents where they have to put digital signatures.

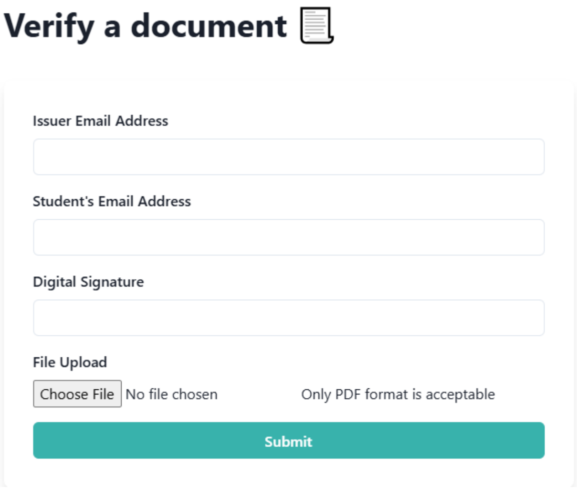
In Figure 6, you can see an student dashboard figure illustrating that students can see their documents which are issued by university.



You have Issued 10 Certificates

NAME	CID	ISSUED TO	LINK TO CERTIFICATE
K196Y43ApplicationForm.pdf	bafybeidgw4mmu4sf324ptzsdop7kj4xqlj3hqgnndwqkcxm2whamco6srq	sad	Download
Neeraj Kumawat _222IT024_M Tech.pdf	bafybeifrib4xejl7kn5b3xdx7hqeaiikhrj72oa6cc6wzeml355nptfjxy	nk12351235123512351235@gmail.com	Download
original_document.pdf	undefined	nkumawat34@gmail.com	Download
original_document.pdf	undefined	nk123512351235@gmail.com	Download
original_document.pdf	bafybeifrlovlhv7ewsrosingkcpsgvnxq54cfdbz5lmaxnfltsencxwudi	nk123512351235@gmail.com	Download

Fig. 4. University Dashboard



Verify a document 📃

Issuer Email Address

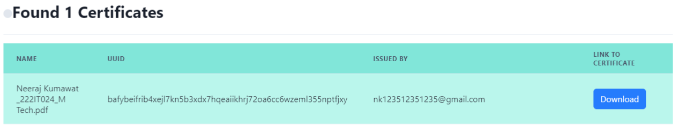
Student's Email Address

Digital Signature

File Upload

Choose File No file chosen Only PDF format is acceptable

Fig. 5. Verification Dashboard



Found 1 Certificates

NAME	UUID	ISSUED BY	LINK TO CERTIFICATE
Neeraj Kumawat _222IT024_M Tech.pdf	bafybeifrib4xejl7kn5b3xdx7hqeaiikhrj72oa6cc6wzeml355nptfjxy	nk123512351235@gmail.com	Download

Fig. 6. Student Dashboard

XI. CONCLUSION AND FUTURE WORK

To improve the verification process, a block chain-based approach for the verification of graduation certificates was put forth in this study. This will lessen the likelihood of certificate fraud and provide enhanced security, legitimacy, and privacy of graduation certificates. Numerous advantages are provided by the suggested model to the issuing authorities, recipients, and customers. The suggested solution has the benefit of having all the data needed to authenticate and validate the certificate stored on the blockchain. The potential employer doesn't even need to get in touch with the university to authenticate the credential. It only has to make sure that the hash produced by the verification. It only has to make sure that the digital signature's hash and the university-issued key match each other. The verification software and key must match for the digital signature to be accepted. The suggested paradigm will be used and taken up in a few chosen academic institutions for subsequent development. It will eventually be expanded to use smart contracts as its foundation.

In future work, emphasis will be placed on integrating digital signature embedding into PDF documents. Additionally, research will be conducted to explore additional encryption methods for securing documents, as well as investigating various approaches for document verification.

REFERENCES

1) Online Document Verification Using Blockchain by Abhijeet Gupta, Chetan Khobragade, Mrudul Gaidhane, Chetan Pawar (June 2023).
2) Blockchain based document verification system by Mayuresh Chaudhari, Kondaka Lakshmisudha (November 2023).
3) Verifi-Chain: A Credentials Verifier using Blockchain and IPFS by Tasfia Rahman, Sumaiya Islam Mouno, Arunangshu Mojumder Raatul, Abul Kalam Al Azad, and Nafees Mansoor (11 Jul 2023).
4) ENHANCING SECURITY AND TRANSPARENCY: THE ROLE OF BLOCKCHAIN IN DOCUMENT VERIFICATION by Kalpita Vilas Birhade, Nitesh Sopan Wani, Sahil Vijay Bhosale, Prathmesh Yuvraj Jadhav, Shantanu Samir Raje (December 2023).
5) Digital Certificate Verification Using Blockchain Technology by Khushal Y. Bheke, Aniket R. Misal, Nilkanth S. Pokharkar, Prof. Gunjal T. S. (May 2023).
6) A Graduation Certificate Verification Model via Utilization of the Blockchain Technology by Osman Ghazali and Omar S. Saleh (2019).
7) Digital Certificate Verification using Blockchain by Muhammad Dhiyaul Rakin Zainuddin and Kan Yeep Choo (Nov 2022).
8) Generating and Validating Certificates Using Blockchain by T.S.Raja Rajeswari, Sk Khaja Shareef, Sameer Khan, N Venkatesh, Akhtar Ali, V. Sri Monika Devi (2021).
9) A novel semantic blockchain-based authentication system of educational certificates by Minh Duc Nguyen, Cuong H. Nguyen-Dinh, Le Anh Phuong (19th Aug 2022).
10) Multi-Format Document Verification System by Madura Rajapashea, Muammar Adnanb, Ashen Dissanayakac, Dasith Guneratned, Kavinga Abeywardane (December 2020).