IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Document Verification And Management System Using Blockchain

Gaytri Kumari[1], Prajwalita Dongre[2], Tiya Mukherjee[3], Pandey Nidhi Mataprasad[4]
[1,3,4]UG Student, [2]Professor
[1,2,3,4]Computer Engineering Department,
Sinhgad Academy of Engineering, Pune, Maharashtra, India

Abstract: Documents and certificates are crucial for proving professional achievements, making them essential for career progression. The current system for issuing and verifying these documents is often slow and labour-intensive. Moreover, paper-based documents are susceptible to forgery, resulting in various educational frauds. This project aims to resolve these issues by leveraging blockchain technology. Blockchain extends beyond cryptocurrencies and has significant applications in various fields, including healthcare, supply chain management, and finance. In education, blockchain can transform the traditional method of issuing and verifying certificates. This project will illustrate how professional certificates can be authenticated using the Ethereum platform and smart contracts. The process includes converting traditional paper certificates into digital formats upon request, applying cryptographic hash functions to generate hash values for the digital certificates, storing the hash values on the blockchain, creating a unique certificate ID and transaction hash value, and utilizing the unique certificate ID and transaction hash value for certificate verification through a unified platform. This approach includes streamlining the certificate issuance, storage and verification process, increasing security by preventing forgery and unauthorized modifications, providing a clear and immutable record of certifications, and facilitating easy access and verification by third parties.

Index Terms **- Blockchain, Document, Storage, Security, Ethereum, Hash Function.**

I. INTRODUCTION

The concept of blockchain technology was first described by research scientists Stuart Haber and W. Scott Stornetta, but it became popular in 2009 when Bitcoin was invented by Satoshi Nakamoto. Blockchain technology is now widespread in the educational sector for many use cases, including issuing and verifying documents (e-transcripts), cost-effective large-scale file storage, automated learning platforms, publishing and copyright protection, and payment via cryptocurrencies. Document verification using blockchain is a project powered by the Ethereum Blockchain, which stores and manages student documents. The management process is end-to-end, encompassing both the issuing of documents and their verification. The platform allows the issuer, typically an institution, to issue documents for an entity, which can then use those documents stored on the network to view and verify for authentication and information verification. Blockchain is a distributed ledger and public system that allows for safe and transparent transaction capturing and affirmation. Its distinguishing characteristics, such as irreversibility, transparency, and decentralization, make it an ideal platform for online document verification. By using blockchain, it is possible to establish an encrypted and tamper-proof record of documents, ensuring their integrity and authenticity. This approach provides a more effective and cost-efficient solution while also enhancing security and reducing the likelihood of fraud and errors by blocking fraudulent IDs. In addition to verification, the system offers the feature of storing and retrieving documents using the Inter Planetary File System (IPFS). The documents are stored on IPFS, with their hash values stored on the blockchain, and the backend coding is implemented using smart contracts.

II. LITERATURE REVIEW

In "Blockchain Based Verification of Educational and Professional Certificates", The proposed system uses Blockchain technology through the use of public Blockchain and smart contract along with a distributed peer to peer storage called IPFS to store the documents. Published by Anjali Singh, SPS Chauhan, Amit Kumar Goel Professor, School of Computing Science and Engineering, Galgotias University Greater Noida, India.
MIT(Massachusetts Institute of Technology) has achieved issuance and verification of certificates through an application known as Blockcerts using the Bitcoin blockchain. Hashes are generated for every batch of certificates and then they are issued in the blockchain. The website then allows the certificates to be printed using JSON objects.
In "Block Chain Based Document Management System" published in 2001, create an API that is much easier to use and share documents. The system can handle all of the necessary steps for setting up Hyperledger, while also allowing users to write simple API calls for requesting documents, creating documents, adding entries to documents, and giving consent to use a specific type of document. Users will be able to utilize a simpler UI on a website to access the same type of API that allows them to simply create new documents and manage UAC (User Access Control).
"A Blockchain Based Authentication System for Digital Documents" has focused on document verification, while document verification is an important aspect of document management, it is not the only consideration when it comes to managing complex document workflows. Document management systems that only focus on document verification may not be sufficient for organizations that require more granular control over document workflows. By exploring document management systems that offer more advanced workflow management capabilities, organizations can ensure that their document management processes are efficient, secure, and tailored to their specific needs.
The authors from University of Jordan have proposed a system called SmartCert that will be used to issue the certificates as well as verify them using smart contracts. There are two parts of this system, User who can use the national ID to view the certificates and Owner of the contract can create a new certificate. The system works in the following way- If the national ID is invalid then the expected output would be student not found. If the student national ID is valid then the certificate ID number and other details would be the output.

III. METHODOLOGY

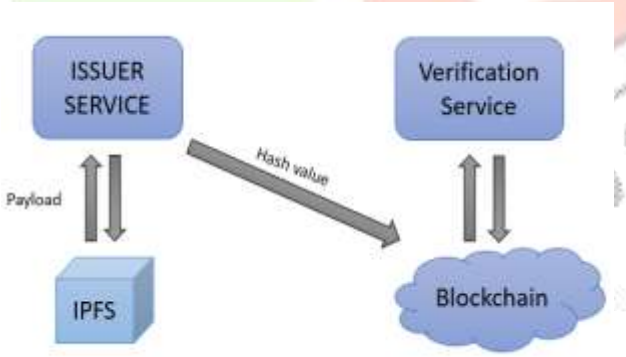

Figure 1: Project Block Diagram

This is a project that aims to implement an efficient anti-forgery mechanism for documents, such as mark sheets, transcripts, diplomas, official identification certificates and other certificates. The goal is to ensure the authenticity of documents, reducing the incidence of counterfeit them, and saving time and financial resources for all parties involved in document verification.
The solution proposed by the project revolves around three roles or entities: **An Issuer, a Verifier, and a User**.

- The issuer is the authority that creates and issues the electronic version of the certificate or document
- Verifier is the potential employer or any person who wants to verify the authenticity of the certificate provided by the user.
- Finally, the user is the recipient of the certificate and can only view the documents issued to him/her.

This is a project that provides an efficient anti-forgery mechanism for documents. By using a combination of blockchain, IPFS, and hash functions, the authenticity of the certificate can be ensured, reducing the incidence of counterfeit certificates and saving time and financial resources for all parties involved in document verification.

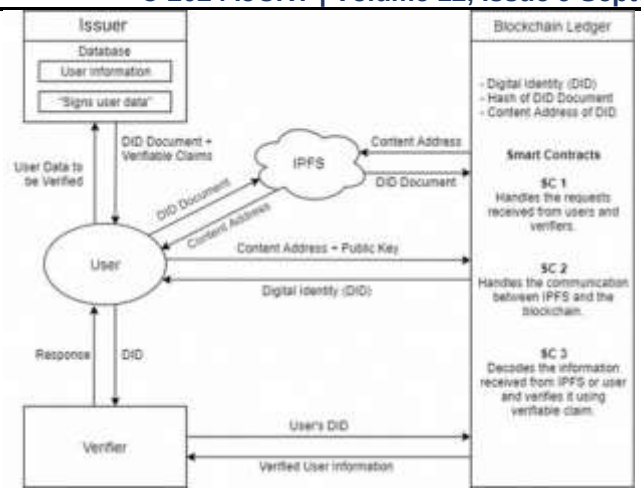

Figure 2: Project Workflow

1. User Registration:
   - User: The user provides his data to the Issuer.
   - Issuer: The issuer captures his data and forms a DID on the database.
   - DID Document: The issuer creates a DID document having the user's data, verifiable claims, and a Content Address.
   - IPFS: This DID document then gets stored on a decentralized data storage network called Inter Planetary File System.

2. Verification Request:
   - Authentication of Claim: The authenticating party sends an authentication request to validate the identity of the user.
   - Recovery of DID Document: The authenticating party retrieves the DID document of the user via its content address using IPFS.

3. Communication with Smart Contract:
   - Smart Contract 1:It is a smart contract that the authenticating party communicates with on the blockchain.
   - Handle Request: Smart Contract 1 receives the authentication request and retrieves the desired information from the DID document.

4. Interaction with IPFS:
   - Smart Contract 2: Smart Contract 2 makes a query to IPFS to retrieve the DID document by its content address.
   - Data Retrieval: The DID document is retrieved from the IPFS, and it sends back to Smart Contract 2.

5. Verification Process:
   - Smart Contract 3: Smart Contract 3 decodes the DID document information and verifies that through verifiable claims.
   - Verification Result: When verification is successful, Smart Contract 3 responds positively to the verifier.

6. Reply to Verifier:
   - Smart Contract 1: Smart Contract 1 returns the outcome of verification back to the verifier.

7. Authentic User Information:
   - Verifier: The verifier gets the outcome of verification and if all good then retrieves the authentic user information.

IV. Comparison And Analysis

Feature	Traditional System	Digital System	Blockchain based System
Storage	Physical storage (e.g., filing cabinets)	Cloud-based storage	Decentralized storage on blockchain and IPFS
Accessibility	Limited to physical location	Accessible from anywhere with internet	Accessible from anywhere with internet
Security	Susceptible to physical damage, theft, and unauthorized access	Less susceptible to physical threats but vulnerable to cyberattacks	Highly secure due to immutability of blockchain and distributed nature of IPFS
Tamper-Proofing	Can be altered or forged	Can be altered or forged, but changes can be detected	Tamper-proof due to the cryptographic nature of blockchain and IPFS
transparency	Limited transparency	Increased transparency through audit trails	High transparency due to public nature of blockchain
Efficiency	Manual processes, time-consuming	Highly efficient due to automation and distributed nature	Highly efficient due to automation and distributed nature

Table 1: Traditional System V/S Digital System V/S Blockchain Based System

V. Discussion

Key features: -

- Immutability: After the documents have been recorded on the blockchain, they cannot be modified, ensuring integrity in data.
- Decentralization: No singular authority has control over the system, thereby reducing the risk of potential tampering or loss of data.
- Transparency: All the actions on the blockchain can be traced, therefore providing verifiable audit trails.
- Security: Cryptographic techniques are applied for securing the documents so that any unauthorized access or forgery of them can become almost improbable.
- Authentication: Third-party instant document authentication via any third party without a central authority.
- Smart Contracts: Automate the workflow and process, such as approvals, based on rules established beforehand.
- Access Control: Access is role-based. Hence, only access for which people are authorized can view or modify the documents.
- Cost and Time Efficiency: It reduces paperwork and manual verification. It accelerates the process and saves cost.

Assumptions: -

- The blockchain platform i.e. Ethereum is stable and scalable to handle the expected workload
- Users will be willing to adopt the new system.
- The system can handle various document formats (PDF, Word, Excel, etc.) and metadata.

Dependencies: -

- The development of smart contracts to govern document creation, modification, and access.
- Sufficient storage capacity to accommodate document data on the blockchain.

VI. Conclusion

This paper has solved main shortcomings in the existing method of certificate issuance, verification and storage by the concerned parties. The proposed system provides the features of immutability, decentralization and tamper-proof documents which can be verified directly without the need of a third party. Firstly, the scam of fraud certificates since in Blockchain it is easy to trace back the transactions, secondly, this method is faster as compared to the existing method involving paper certificates and finally providing the distributed storage of document using IPFS. The Blockchain technology allows the generation of e-certificates with unique hash values which are then further used to verify the certificates. The unique hash values corresponding to each certificate makes this system more secure and forgery proof.

VII. Acknowledgment

We would like to extend our gratitude to Project staff at the Sinhgad Academy of Engineering, Department of Computer Engineering for their immense support and help without which this work could not have been accomplished. Additionally, we would like to give Mrs. Prajwalita Dongre, our project manager, our profound gratitude for guiding us through the process.

References

[1] Anjali Singh, SPS Chauhan, Amit Kumar Goel Professor, School of Computing Science and Engineering, Galgotias University Greater Noida, India, "Blockchain Based Verification of Educational and Professional Certificates",2023, DOI: 10.1109/ICCSC56913.2023.10143008

[2] SHINYA HAGA AND KAZUMASA OMOTE Faculty of Engineering, Information and Systems, University of Tsukuba, Tsukuba 305-8577, Japan, “Blockchain-Based Autonomous Notarization System Using National eID Card " ,2022, DOI 10.1109/ACCESS.2022.3199744

[3] Mr. S. CHOUDAIAH, Mr. U. CHANDRASELHAR, Dept of MCA, SVEC - Sree Vidyanikethan Engineering College, Tirupati, “Block Chain Based Document Management System”, Vol 12, Issue 08, August/2021 ISSN NO:0377-9254

[4] Yerramsetti Sri Uday Kiran Sai Mahesh, Velagapudi Rohith, Vennam Srinivas Reddy , Mrs B. Ratnamala, Dr. Reddyvaari Venkateswara Reddy, "A review on Student Document Management System based on Ethereum Blockchain (PERSONAL- D)", ISSN: 2278-0181 Vol. 12 Issue 08, August-2023

[5] Prof. Renuka Vaidya, Ms. Sanskriti Punde, Mr. Kartikey Yadav, Mr. Chakradhar Ghute, Ms. Namrata Shinde Assistant Professor, Department of Information Technology Students, Department of Information Technology Sinhgad College of Engineering, Pune, India, “Document Management System using Blockchain”, Volume 3, Issue 13, May 2023, DOI: 10.48175/568

[6] Moumita Das, Jack C. P. Cheng, Xingyu Tao, “A Secure and Distributed Construction Document Management System Using Blockchain”, January 2021 DOI: 10.1007/978-3-030-51295-8_59

[7] Sakshi Jha, Govind Dhingra, Gagan Mittal, Harsh Vardan, Department of Computer Science and Engineering, Maharaja Agrasen Institute of Technology, Delhi, India “Secured Document Storing Using Blockchain”, 2022 IJRTI, Volume 7, Issue 5, ISSN: 2456-3315