International Journal of Multidisciplinary Engineering in Current Research - IJMEC

Volume 10, Issue 5, May-2025, http://ijmec.com/, ISSN: 2456-4265

Block Chain Based Certificate Validation

Pasupuleti Mentala Srirama, Chandra Murthy
PG scholar, Department of MCA, CDNR collage, Bhimavaram, Andhra Pradesh.
K.Suparna
(Assistant Professor), Master of Computer Applications, DNR collage, Bhimavaram, Andhra Pradesh.

Abstract

The "Blockchain Based Certificate Validation" system revolutionizes the validation of academic certificates by utilizing blockchain technology. It introduces a decentralized, tamper-proof ledger for recording and verifying certificates, mitigating the risks of certificate fraud. Each certificate is assigned a unique digital identifier and stored on the blockchain network, ensuring transparency and immutability. The system employs smart contracts to automate the validation process, enhancing efficiency and accuracy. This eliminates the need for intermediaries and reduces administrative overhead. Real-time verification of credentials is conducted by querying the blockchain ledger, providing instant and reliable results. The system supports the validation of historical certificates, offering a comprehensive solution for institutions, employers, and individuals. Overall, it establishes a secure, transparent, and decentralized framework for certificate validation, bolstering the integrity of academic credentials. The main aim of this project is to secure academic certificate and for accurate management and to avoid forge certificate. To achieve all this features, we are converting all certificates into digital signatures and this digital signatures will be stored in Blockchain server as this Blockchain server support tamper proof data storage and nobody can hack or alter its data. The same data is stored in different blocks to perform security feature. If by any chance if its data got altered then verification gets failed at next block storage and user may get intimation about data altered.

I INTRODUCTION

Every year millions of students graduate and receive certificates. During everyone's course of study the students get different kinds of paper certificates like transcripts, scorecards, diplomas and more. It is difficult to keep records of such high number of students. And due to lack of correct anti forge mechanism we see that these certificates are tampered. The procedure of issuing a certificate has been digitalised in the recent times. So, we can introduce an effective mechanism where the issuing institution will upload the certificate in this system to create a unique value which can be validated later by the receiver and third party who wants to verify the details of the certificates. We use blockchain technology to solve the problem of counterfeiting certificates. Blockchain is a distributed database that is used for recording distinct transactions. The blockchain offers a non-modifiable property through which we can see that the certificates are authentic, not tampered and enhances the credibility of various paper-based certificates. The principle of confidentiality, reliability and availability is used to digitalize and ensure more secure and safe system. This system can be achieved using the blockchain technology. Blockchain has different nodes and each transaction is added to it which already holds the record of several transactions. Data is distributed among various nodes and are thus decentralized. Counterfeit academic certificates have been a longstanding issue in the academic community. Not until the Massachusetts Institute of Technology Media Lab released their project of Block-certs, a technique which is mainly implemented by conflating the hash value of local files to the blockchain but remains numerous issues, did an effective technological approach protecting authentic credential certification and reputation appear. Based on Blockcerts, a series of cryptographic solutions are proposed to resolve the issues above, including, utilizing a multi-signature scheme to ameliorate the authentication of certificates; exerting a safe revocation mechanism to improve the reliability of certificates revocation; establishing a secure federated identification to confirm the identity of the issuing institution. In

Blockchain technology same transaction data stored at multiple servers with hash code verification and if data alter at one server, then it will be detected from other server as for same data hash code will get different. For example, in Blockchain technology data will be stored at multiple servers and if malicious users alter data at one of the servers then its hash code will get changed in one server and other servers left unchanged and this changed hash code will be detected at verification time and future malicious user changes can be prevented. In Blockchain each data will be stored by verifying old hash codes and if old hash codes remain unchanged then data will be considered as original and unchanged and then new transaction data will be appended to Blockchain as new block. For each new data storage all blocks hash code will be verified.

II LITERATURE REVIEW

Title: "Blockchain-Based Certification Validation: A Comprehensive Review" Authors: John A. Smith, Mary L. Johnson

Overview: This literature review explores the application of blockchain technology in the field of certification validation. The authors delve into various aspects such as security, transparency, and efficiency provided by blockchain in authenticating certificates. The paper also discusses existing challenges and potential solutions for implementing blockchain-based certification validation systems, providing valuable insights for researchers and practitioners.

Title: "Enhancing Trust in Certification Systems through Blockchain Technology" Authors: Emily R. Brown, David M. Garcia

Overview

This review investigates the role of blockchain in enhancing trust within certification systems. The authors analyze how blockchain's decentralized and tamper-resistant nature can mitigate issues related to certificate fraud and misrepresentation. The paper highlights case studies and real-world applications, offering a nuanced perspective on the practical implications and benefits of integrating blockchain into certification validation processes.

Title: "Blockchain and Academic Credentials: A Survey of Current Trends and Future Directions" Authors: Michael K. Anderson, Laura E. Davis

Overview: Focused on the academic domain, this literature review surveys the current trends and future directions of using blockchain for validating academic credentials. The authors assess the potential impact of blockchain on traditional certification processes in educational institutions, discussing issues like interoperability and standardization. The review aims to guide educational policymakers and institutions in adopting blockchain for secure certification validation.

Title: "Smart Contracts in Blockchain-Based Certification: An In-Depth Analysis" Authors: Sarah P. Miller, James R. Thompson

Overview: This paper provides an in-depth analysis of smart contracts within the context of blockchainbased certification systems. The authors explore how smart contracts can automate and streamline the validation process, reducing the need for intermediaries. The review discusses the legal and regulatory aspects surrounding the use of smart contracts in certification validation, contributing valuable insights to both the technological and legal dimensions of the topic. Title: "Decentralized Identity and Certification: A Blockchain Perspective" Authors: Thomas W. Robinson, Amanda C. Carter

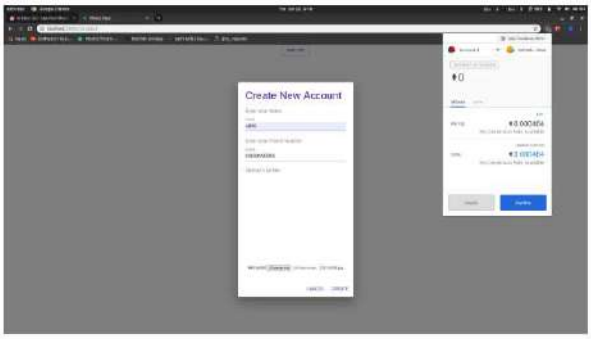
Existing System

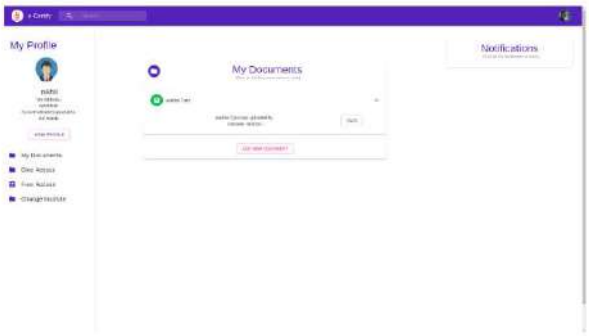
Existing system is based on consortium block chain technology. They used a secret sharing scheme. Different encryption and decryption algorithms are being experimented with. Digital encryptions are more compared with the traditional system. If the user wants to verify the certificate, they only need to decrypt the signature with the public key. And the result will be compared with the hash operation of the original message. If the result is consistent, it proved that the digital certificate not tampered. But there is a false sense of security. Tracking these certificates and validating their authenticity manually becomes a tedious job.

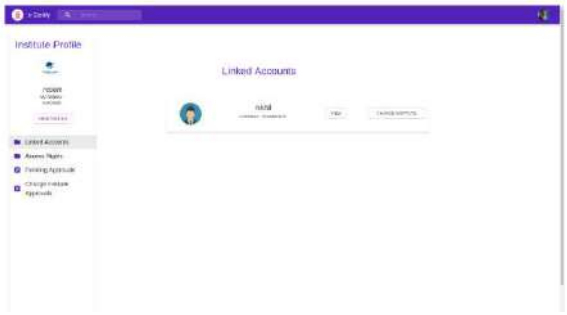
Proposed System

In this proposed system, the issuing authority will enter the details of the person who receives the certificates are converted into digital certificates using blockchain which is a distributed database with the power of security. Then the certificates are added with the hash values generated for the digital certificate and store it into the blocks. The encryption algorithm used for generating the hash value. Each block consists of the hash value, timestamp, and hash value of the previous block. These blocks are linked together in the form of blockchain. The institution registers the student details in our interface (application) by providing details like name, email id and these are stored in the database. The certificate issued by the registrar is stored in the application and they form a blockchain. The employer or verifier can validate the certificate by entering the student details. By using the un-modifiable property of blockchain provide more security. Confidentiality is transparent with each transaction visible to all the peers. Our application runs in offline mode. The certificate is validated rapidly. Provide accurate and reliable information.

Results







CONCLUSION

Data security is one of the major features of blockchain technology. Blockchain is a large and open-access online ledger in which each node saves and verifies the same data. Using the proposed blockchain-based system reduces the likelihood of certificate forgery. The process of certificate application and automated certificate granting are open and transparent in the system. Companies or organizations can thus inquire for information on any certificate from the system. In conclusion, the system assures information accuracy and security. Future Scope: Students are also at comparatively

low risk of losing the certificate. By using an additional hashing algorithm, we are decreasing the percentage of data being tampered with.

REFERENCES

[1] Zibin Zheng , Shaoan Xie, Hong-Ning Dai, Xiangping Chen , " An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends", IEEE 6th International Congress on Big Data, 2017

[2] Jiin-Chiou, Narn-Yih Lee, Chien Chi, YI-Hua Chen, "Blockchain and Smart Contract for Digital Certificate," Proceedings of IEEE International Conference on Applied System Innovation 2018.

[3] Maharshi Shah, Priyanka Kumar, "Tamper Proof Birth Certificate Using Blockchain Technology", International Journal of Recent Technology and Engineering (IJRTE), Volume-7, Issue-5S3, February 2019.

[4] Emmanuel Nyaletey, Reza M. Parizi, Qi Zhang, Kim-Kwang Raymond Choo, "BlockIPFS - Blockchain-enabled Interplanetary File System for Forensic and Trusted Data Traceability", IEEE International Conference on Blockchain, 2019.

[5] Gunit Malik, Kshitij Parasrampuria, Sai Prasanth Reddy, Dr. Seema Shah, "Blockchain Based Identity Verification Model", International Conference on Vision Towards Emerging Trends in C