IJFANS INTERNATIONAL JOURNAL OF FOOD AND NUTRITIONAL SCIENCES
ISSN PRINT 2319 1775 Online 2320 7876
 UGC CARE Listed (Group -I) Journal Volume 12, Iss 4, 2023

Block Chain Based Certificate Validation

G.Jahnavi1,Nagaram Bhavana2,Dathrik Sai Priya3,Mrs.M.Prathiba4

Assistant Professor,Email:swecprathibait@gmail.com
1, 2, 3, 4 Sridevi Women's Engineering College, V.N.PALLY , NEAR WIPRO
GOPANANPALLY, HYDERABAD, Ranga Reddy, 500075 ; Email : admin@swec.ac.inWebsite,
www.swec.ac.in ;

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.

Keywords: Blockchain, Certificate Validation, Decentralized Ledger, Cryptography, Smart Contracts, Digital Credentials, Authentication, Distributed Ledger Technology, Secure Verification, Credential Transparency.

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

ISSN PRINT 2319 1775 Online 2320 7876
 UGC CARE Listed (Group -I) Journal Volume 12, Iss 4, 2023

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 blockchain-based 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

Overview:

ISSN PRINT 2319 1775 Online 2320 7876
 UGC CARE Listed (Group -I) Journal Volume 12, Iss 4, 2023

Focusing on decentralized identity, this literature review examines the role of blockchain in reshaping certification processes. The authors discuss the potential of blockchain to empower individuals with control over their own credentials and the implications for privacy and security. The paper also addresses challenges such as scalability and user adoption, offering a comprehensive overview of the evolving landscape of decentralized identity and certification validation.

III SYSTEM ANALYSIS

1 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.

Disadvantages

- Relies on consortium blockchain technology and secret sharing scheme.
- Utilizes various encryption and decryption algorithms for security.
- Employs digital encryption methods, which are more advanced than traditional approaches.
- Verification of certificates involves decrypting the signature with a public key and comparing it with the original message's hash.
- However, there is a potential false sense of security, and manual tracking and validation of certificates can be laborious.

2 Problem Statement

The existing system relies on consortium blockchain technology and a secret sharing scheme for certificate validation. While various encryption and decryption algorithms are employed, there is a potential false sense of security. Additionally, the manual tracking and validation of certificates become laborious and time-consuming. In the proposed system, the issuing authority converts recipient details into digital certificates using blockchain, ensuring a high level of security. These certificates are enhanced with hash values generated through encryption algorithms and stored in blocks. Each block contains crucial information like hash value, timestamp, and the previous block's hash value, forming a secure blockchain. The system also allows institutions to register student details in an application, providing a reliable database. Certificates issued by the registrar are stored in the application and added to the blockchain.

3 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.

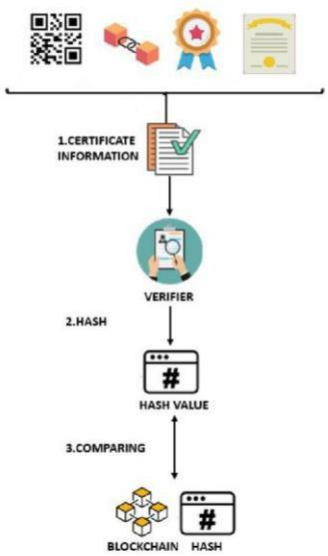
Advantages

- The issuing authority inputs recipient details to generate digital certificates using blockchain, ensuring security.
- Certificates are appended with hash values generated through encryption algorithms and stored in blocks.

ISSN PRINT 2319 1775 Online 2320 7876
Research paper UGC CARE Listed (Group -I) Journal Volume 12, Iss 4, 2023

- Each block contains hash value, timestamp, and the previous block's hash value, forming a blockchain.
- Institution registers student details in the application, including name and email, which are stored in the database.
- Certificates issued by the registrar are stored in the application and added to the blockchain.
- Employers or verifiers can validate certificates by entering student details, leveraging the unmodifiable nature of blockchain for enhanced security.
- Offers transparency, as all transactions are visible to peers, ensuring confidentiality.
- Operates in offline mode, ensuring rapid certificate validation with precise and reliable information.

4 System Architecture



Proposed Architecture

IV IMPLEMENTATION

To establish a blockchain-based certificate validation system, a meticulous methodology is essential, beginning with a comprehensive analysis of the system's requirements. This entails identifying the specific certificates to be validated, the involved entities such as issuers, recipients, and validators, and the desired security parameters. Following this, a suitable blockchain platform is selected, weighing factors such as scalability, consensus mechanisms, and smart contract capabilities. Notable platforms like Ethereum, Hyperledger Fabric, or Binance Smart Chain may be considered based on project requirements.

The development process involves the creation of smart contracts to manage the certificate validation process. These contracts define the structure of certificates, set validation rules, and include functions for certificate issuance and validation. A decentralized identity management system is also implemented, allowing for unique identification of users and entities through standards like Decentralized Identifiers (DIDs) and Verifiable Credentials.

Certificates are then issued and digitally signed by the respective authority, with each certificate assigned a unique identifier and relevant metadata. The subsequent step involves the setup of a private or consortium blockchain network, ensuring proper node configuration and network security. Permissions are configured to control access to functions and data on the blockchain.

Certificates are stored as transactions on the blockchain, with the content of certificates stored either on-chain or off-chain based on the platform and privacy considerations. Smart contracts are developed to embed validation rules, enabling validators to query the blockchain to check the authenticity and status of certificates.

User interfaces for certificate issuance and validation are created to provide a user-friendly interaction with the blockchain-based system. Interoperability with existing systems is ensured through the development of APIs or connectors. Permission and access control mechanisms are implemented to restrict actions and data access based on user roles.

Thorough testing, including unit testing, integration testing, and end-to-end testing, is conducted to verify the functionality, security, and performance of the system. Upon successful testing, the system is deployed on the chosen blockchain network, ensuring

operational efficiency and seamless interaction between components.

Education and adoption strategies follow deployment, aiming to familiarize stakeholders with the system's usage and emphasize the benefits of transparency, immutability, and security. The final stages involve setting up monitoring tools for ongoing performance tracking and implementing maintenance procedures for regular updates to smart contracts and addressing any security vulnerabilities or system enhancements. This methodology ensures the development of a robust and effective blockchain-based certificate validation system.

V 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. The Hash of the certificate is being stored in the blockchain while the original document .This will help us preserve the data and create transparency. The entire automated system of certificate generation and verification will enhance the security and reduce the manual risk in the future.

VI 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 Communication and Networking (ViTECoN), 2019.