BLOCK CHAIN BASED IMPROVED CERTIFICATE VALIDATION SYSTEM

Abstract

A student earns numerous certificates throughout the course of their studies, whether they are in high school, college, or after receiving their degree. These certificates could include transcripts, results, or diplomas. In order to get admitted, students must provide these certifications to institutions or businesses. Following these certifications and carefully examining their validity grows laborious. So, we are introducing certificate validation using the block chain process in which we are sorting. E-Certify can assist address the major issue of certificate fraud since it offers a way to protect a certificate's authenticity and operates under the premise that: "Only the issuer can upload the certificate and the rest people can only view it." Together with IPFS, the entire procedure runs on the blockchain (which offers data security). This is a contemporary and hassle-free way to manage certificates and validate them because it does everything for certificates, including storing, validating, and sharing them.

Authors

Ms. B. Parkavi
Assistant Professor
School of Computer Science and Engineering & Information Science
Presidency University
Bangalore, Karnataka, India.

Ms. Mary Divya Shamili. D
Assistant Professor
School of Computer Science and Engineering & Information Science
Bangalore, Karnataka, India.

I. INTRODUCTION

In India, the fundamental format of a student's education is to enrol in kindergarten, then transfer to a different school for primary, middle, and high school studies. Students must now submit an application for junior college admission after graduating from high school. Additionally, there is a second college switch for graduation. This is the fundamental timeline for a student's academic years. Following this, some students decide to pursue their education further. The problem with this progression is that each level requires a student to validate all of his certificates in front of the examiner. The certificate runs the danger of being misplaced or broken, and the validator must laboriously authenticate each certificate.

II. LITERATURE SURVEY

In today's digital age, everything is digitalized, including academic certificates like the SSLC and HSC that are given to students in educational institutions. It is challenging for students to hold onto their degree diplomas. Verification and validation of credentials are time-consuming and difficult for the organisation and institution. Our project will contribute to the secure storage of the certificate in the blockchain system. Paper-based certificates are first transformed into digital ones. The encrypted value for the certificate is created using the chaotic algorithm. The certifications are then kept on the blockchain. And the mobile application is used to validate these certificates. We can deliver a more effective and safe digital certificate validation using blockchain technology.[1]

Mobile devices have the ability to both use and offer services. As per the OMA mobile Web services specifics, they do indeed function as a peer. It is a change from simple data sharing to the full delivery of application services to smartphones and tablets. Due to the fact that devices could be assigned to a number of trusting domains without a formal relationship being established, digital certificates might be used to confirm the supply of services.In addition to interoperability problems, PKI adoption is expanding and entering new environments. However, the cost of creating and certifying the certification channels falls on programmes that use such certificates. Due to wireless communications, limited processing capacity, and higher costs than permanent infrastructure networks, these procedures may become more complicated and expensive. Different strategies for delegating certificate validation and simplifying the process of receiving status information have been established by the IETF PKIX WG. Mobile devices do not, however, yet support these. For these reasons, we suggest creating an open toolset based on OpenSSL for validating X.509 public key certificates. PDAs are being used to successfully create and test this toolbox.[2]

Academic credentials are crucial to a person's job, making them more vulnerable to fraud. The idea of exchanging certificates and using blockchain technology to confirm their authenticity is put out in this paper. Information sharing and safe data storage are made possible by blockchain technology. Trust among users is its key priority. Using Hyperledger Fabric, this proposal focuses on creating and constructing a system that would serve as a remedy for the problem of fraudulent certificates. The technology used here is transparent and impervious to tampering. This system will have a database of academic certificates granted by the University that are recorded as transactions using the Hyperledger Fabric. Other organisations present in the network can refer to this database to verify the authenticity of the certificates using the data supplied by the students. Encryption is offered end to end by this technology.[3]

This study aims to build a public blockchain-based system for document storage for job training. In order to safeguard certificate data, public platforms are employed, making falsification harder. Data that will be included in blocks broadcast to the Ethereum blockchain network is created through the use of smart contracts. In a distributed setting, certificate files are kept using the InterPlanetary File System (IPFS) to make accessing them simple and secure. The findings demonstrated that certificate data can be kept on public blockchain Ethereum infrastructure, along with its supporting files, and that this data can also be kept in an IPFS environment. This indicates that because certificate data is maintained in a decentralised and open blockchain environment, it is more protected against forgery.[4]

Public key infrastructures (PKIs) for certificate authentication now in use have a number of security issues. Any domain name is eligible for a certificate from a reputable certificate authority (CA) that is legitimate. Despite the fact that a client is supposed to trust a CA if the certificate they obtain is connected to the chain of trust (for instance, the root CA or a subordinate CA). The security of the system as a whole is at risk if an attacker manages to breach any of the latter (for instance, root CAs or subordinate CAs). Additionally, domain owners must have faith in independent CAs. The level of trust between the parties engaged in certificate authentication and issuance, such as CAs and domain owners, is currently unbalanced. Techniques like Domain Authentication Name Entity (DANE) and Certificate Authority Authorization (CAA) increase the security of domain authentication in order to solve this issue. These techniques, however, are dependent on the DNS/DNSSEC infrastructure, which has a low acceptance rate and demanding setup procedures. In this work, we propose and develop a trustworthy and scalable domain authentication technique based on blockchain technology with privacy-preserving features for low-constrained devices (such as mobile, browser, and IoT devices). The proposed system keeps a list of trusted CAs, each one associated with a certain domain, in the blockchain. To put it another way, each CA must first decide if it can be relied upon to manage the actual issuance process. To show how much less disc space and bandwidth our system requires in comparison to other approaches to authenticate certificates, we compare it to different authentication strategies.[5]
Published in:

The Internet of Vehicles (IoV) study trend has led to an increase in interest in concerns regarding the security vulnerabilities privacy of each internet automobile. To lower the cost of safely validating certificates, we put our attention on certificate administration. The management and dissemination of the Certificate Revocation List (CRL) in the vehicle public key infrastructure (PKI) are addressed in this article using blockchain technology. Our suggested method relies on time to a non-revoked vehicle for a blockchain system to validate the certificate using activation codes. The cost of verification will be decreased, and the certificate for inactive cars will automatically be removed.[6]

III. PROPOSED METHODOLOGY

1. In this project we have two ways for login they are :

- Student login
- Institute login

In Student login side student should connect to there institute by giving institute address key and once the student account is created he will get the option to upload the

certificate and that certificate will appear only after approval of the given institute, once the approval is given from the institute side the certificate will be visible on the dashboard of the student.

Student can share/give access to other institute/organization to his / her certificates only after then the certificated will be visible for other organization
In the student login side we have another option for change of institute request in which student can send the request of change of institute for the current institute once the approval is given from the current institute the institute will be changed.

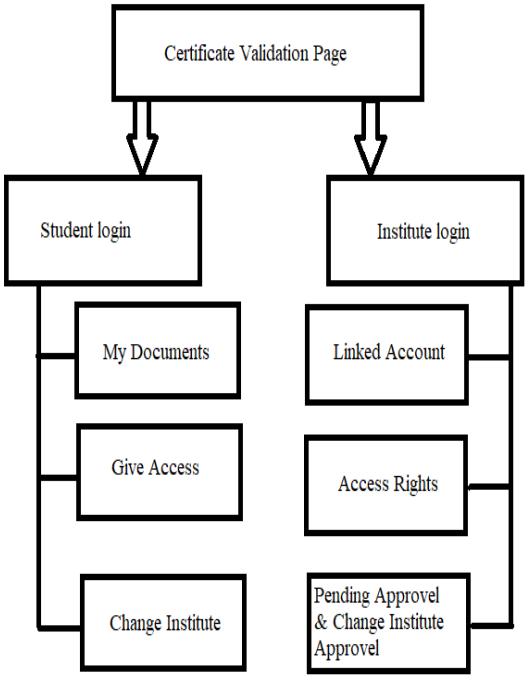
2. **In Institute Login Side**: in this dashboard we have student accounts which are trying to link there account with institute are shown in this dashboard, and also students certificate will be shown here and institute can also add there new certificates here for the students, all the certificated students have uploaded in there dashboard are shown here and it also shown for which certificate institute has the access to view the request for approval of certificate from the student will be shown in the institute dashboard for which the institute can view that certificate and verify that certificate like this the students certificate is verified by the institute.

   Change of institute request will be appear in the institute dashboard for which institute can view the students details and he can approve or disapprove the request of the student to change his institute

3. **Ease of Use**

- To build the E-certificate system which reduces the problem of verifying the certificate
- To build the system which stores the certificate in decentralized way using Block-chain system
- To build the system in which student should upload the certificates and institute should verify that certificate
- To build the system in which verified certificated can be shared with originations / institutes
- To build the system in which student dashboard and Institution dashboard should be created and students can upload there certificated, and institutes can verify that certificates

IV. ARCHITECTURE DIAGRAM



Existing Methods: In the existing system our marks cards and certificates are stored and preserved in the colleges and institutes in which we are currently pursuing our education, so our documents are stored in hardcopy in our institutes or in university

V. CONCLUSION

The ability to create immutable ledgers is one amongst Blockchain's primary features. This behaviour assists us in creating a system where all processes are open and unalterable. Our System automates the creation of certificates and minimises the amount of manual labour required for their verification. Additionally, there is a comparatively low chance of certificate loss for students. We are reducing the amount of modified data by employing an additional hashing technique. The certificate's hash is retained on the blockchain, while the real documents will be kept preserved in the Inter Planetary File System (IPFS). This will assist us in maintaining the data and fostering transparency.

1. Drawbacks of Existing System

- the certificates and marks cards are stored in our univer- sity or in our institutes can be lost or can be missing
- the certificates will not be available for the students on time when they require it because it will be in out institutes or in our colleges
- the certificates can be manipulated or can be forgery by students because it is a hardcopy
- the person or a student should carry bunch of certificates or marks cards with him for

an interview and the in- terviewer should waste his time on validating the given certificates is proper or not.

REFERENCES

[1] Gayathiri; J. Jayachitra; S. Matilda, Certificate validation using blockchain, 2020 7th International Conference on Smart Structures and Systems (ICSSS) , https://ieeexplore.ieee.org/document/9201988
[2] Florina Almenarez; Andres Marin; Daniel Diaz; Alberto Cortes; Celeste Campo; Carlos Garcia-Rubio,Building an Open Toolkit of Digital Certificate Validation for Mobile Web Services, 2008 Sixth Annual IEEE International Conference on Pervasive Computing and Communications (PerCom), https://ieeexplore.ieee.org/document/4517456
[3] Academic Certificate Validation Using Blockchain Technology, Garima Sethia; Sambarapu Namratha; Srikanth H; Sreeja C S, 2022 International Conference on Trends in Quantum Computing and Emerging Business Technologies (TQCEBT),https://ieeexplore.ieee.org/document/10041550
[4] Design and Implementation of Work Training Certificate Verification Based On Public Blockchain Platform ,Irawan Afrianto; Yayan Heryanto, 2020 Fifth International Conference on Informatics and Computing (ICIC), https://ieeexplore.ieee.org/document/9288610
[5] LightLedger: A Novel Blockchain-Based Domain Certificate Authentication and Validation Scheme,
[6] Abba Garba; Zhong Chen; Zhi Guan; Gautam Srivastava, IEEE Transactions on Network Science and Engineering (Volume: 8, Issue: 2, 01 April-June 2021),https://ieeexplore.ieee.org/document/9387577
[7] Efficient Certificate Management in Blockchain based Internet of Vehicles,Ei Mon Cho; Maharage Nisansala Sevwandi Perera, 2020 20th IEEE/ACM International Symposium on Cluster, Cloud and Internet Computing (CCGRID),https://ieeexplore.ieee.org/document/9139652

