International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 07 Issue: 05 | May - 2023 SJIF 2023: 8.176 ISSN: 2582-3930

BLOCK-CHAIN BASED CERTIFICATE VALIDATION

Deekshith Kumar CV, NM Afridh, M Junaid, M Junaid, Final Year, CSE,Presidency University and
Ms.B.Parkavi, Assistant Professor, School of CSE & IS, Presidency University

Abstract—A student, whether a high school student, an undergraduate, or a postgraduate, generates many certificates that may include results, diplomas, or transcripts during this entire study duration. For admission, students need to produce these certificates in institutions or companies. Tracking these certificates and validating their authenticity manually becomes a tedious job. So, we are introducing certificate validation using the block chain process in which we are sorting. The major problem of counterfeit certificates can be tackled with the help of E-Certify, as it provides a solution to preserve the genuineness of a certificate.and It works on the idea that: "Only the issuer can upload the certificate and the rest people can only view it." The entire process works on the blockchain in partnership with the IPFS (to provide data security). and it Does Everything for certificates like Storing, Validating, and Sharing and this is a modern and hassle-free solution to manage certificates and verify them

I. Introduction

In India, the basic structure of a student's studies goes like taking admission in kindergarten, after that changing of school for primary, secondary, and high school studies. Now, after completing high school students need to get admission into junior college. For graduation, there's also once again changing of college. This is the basic cycle for a student's study years. After this, some students continue to pursue higher studies. So, the problem with this cycle is that a student needs to produce all his certificates in each stage for validation. This poses a risk of losing and damaging the certificate. And it is tedious for the validator to authenticate each certificate.

literature survey
1.Certificate validation using blockchain

Publisher: IEEE

A. Gayathiri; J. Jayachitra; S. Matilda

Abstract:

In the digital world, each and everything is digitalized in which the certificate of SSLC, HSC, and academic certificate are digitalized in the educational institution and provided to the students. Students are difficult to maintain their degree certificates. For the organization and institution, verification and validation of certificates are tedious and cumbersome. Our project will help to store the certificate in the blockchain system and provide security. First, the paper certificates are converted into digital certificates. The chaotic algorithm is used to generate the hash code value for the certificate. Then the certificates are store in blockchain. And these certificates are validated by using the mobile application. By using blockchain technology we can provide a more secure and efficient digital certificate validation.

Published in: 2020 7th International Conference on Smart Structures and Systems (ICSSS)

https://ieeexplore.ieee.org/document/9201988

2.Building an Open Toolkit of Digital Certificate Validation for Mobile Web Services

Publisher: IEEE

Florina Almenarez; Andres Marin; Daniel Diaz; Alberto Cortes; Celeste Campo; Carlos Garcia-Rubio

Abstract:

Mobile devices can both consume and provide services. They act indeed as a peer, according to the OMA mobile Web services specification. It is a move from simple data sharing to full deliver of application services down to mobile devices. The use of digital certificates to ensure the provision of services is suitable because devices can belong to different trust domains without having previously an established relationship. Besides, by interoperability issues, the use of PKI continues to grow and move into diverse environments. However, applications making use of such certificates are burdened with the overhead of constructing and validating the certification paths. These processes can become more complex and costly than fixed-infrastructure networks due to the wireless communications and restricted processing and power capabilities. The IETF PKIX WG has specified different mechanisms for delegating the certificate validation and making lighter the status information obtaining. However, these are not supported currently by mobile devices. For these reasons, we propose to develop an open toolkit for X.509 public key certificate validating based on OpenSSL. This toolkit is being developed and tested successfully in PDAs.

Published in: 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

Publisher: IEEE

Garima Sethia; Sambarapu Namratha; Srikanth H; Sreeja C S

Abstract:

Academic certificates are essential for an individual's career and hence they are more prone to being tampered. This paper proposes an idea of sharing certificates and verifying their authenticity using blockchain technology. Blockchain paves the way for secure storage and sharing of information. Its main focus is to maintain trust among users. This proposal focuses on designing and implementing a system that will prove to be a solution for addressing the issue of fake certificates using Hyperledger Fabric. The technology here is tamper-proof and maintains transparency. This system will have a database of academic certificates awarded by the University, which is recorded as a transaction using the Hyperledger Fabric, which further can be referred by other organizations present in the network to verify the authenticity of the certificates using the information provided by the students to the database. This system provides end to end encryption.

Published in: 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

Publisher: IEEE

Irawan Afrianto; Yayan Heryanto

Abstract:

The purpose of this research is to develop a job training document storage system based on the public blockchain platform. The use of public platforms is used to secure certificate data making it difficult to falsify. The use of smart contracts is used to form data that will be used in blocks to be sent to the Ethereum blockchain network. The InterPlanetary File System (IPFS) is used to store certificate files in a distributed environment so that access is easy and safe to do. The results showed that certificate data can be stored in public blockchain Ethereum infrastructure and its supporting files stored in the IPFS environment. This means that certificate data is more secure from counterfeiting because it is stored in a distributed and transparent blockchain environment.

Published in: 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

Publisher: IEEE

Abba Garba; Zhong Chen; Zhi Guan; Gautam Srivastava

Abstract:

Nowadays, existing public key infrastructures (PKIs) certificate authentication suffers from many security failures. Trusted certificate authorities (CAs) can issue a valid certificate for any domain name. Although CA is supposed to be trusted by a client if the certificate issued to the client links to the chain of trust (e.g., root CA or subordinate CA). By compromising any of the latter (e.g., root CAs or subordinate CAs) an attacker can jeopardize the security of the entire system. Moreover, third-party CAs have to be trusted by domain owners. Currently, the trust is not balanced among the entities involved in the certificate authentication and issuance process (i.e., CAs and domain owners). To counter this problem approaches such as Domain authentication name entity (DANE) and Certificate Authority Authorization (CAA) offer additional securities for domain authentication. However, these approaches depend upon DNS/DNSSEC infrastructure which requires complex requirements for deployment as well as the adoption rate has been low. In this paper, we design, implement a robust and scalable domain authentication scheme based on blockchain technology with privacy-preserving features for low-constrained devices (e.g., mobile, browser, and IoT devices). The proposed system records a set of trusted CAs each associated with a specific domain in the blockchain. That is, each CA has to first verify if it is trusted to perform the actual issuance process. We compare our scheme with existing authentication methods and show that it requires less storage capacity and low bandwidth to authenticate certificates than other methods.

Published in: IEEE Transactions on Network Science and

Engineering (Volume: 8, Issue: 2, 01 April-June 2021) https://ieeexplore.ieee.org/document/9387577

6.Efficient Certificate Management in Blockchain based Internet of Vehicles

Publisher: IEEE

Ei Mon Cho; **Maharage Nisansala Sevwandi Perera**

Abstract:

Driving to the research trend to the Internet of Vehicle (IoV), the issues of privacy and security of each internet car become popular. We focus on the certificate management to reduce the cost of certificate validation securely. In this paper, we use the blockchain technology to address the distribution and management of the Certificate Revocation List (CRL) in vehicle public key infrastructure (PKI). Our proposed scheme uses the activation codes to validate the certificate depends on time to non-revoked vehicle for blockchain mechanism. We intend to reduce the verification cost and naturally remove the certificate of inactive cars.

Published in: 2020 20th IEEE/ACM International Symposium on Cluster, Cloud and Internet Computing (CCGRID)

https://ieeexplore.ieee.org/document/9139652

PROPOSED METHODOLOGY

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

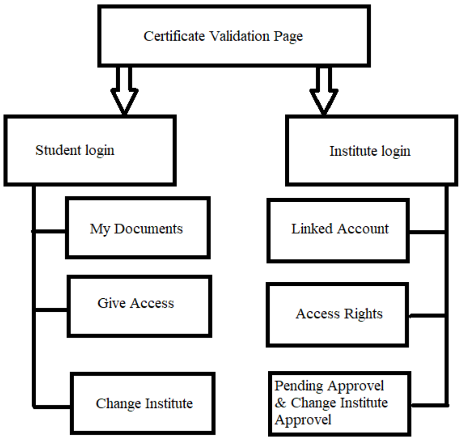
1. Student login
2. Institute login

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.
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

II. EASE OF USE

- To build the E-certificate system which reduces the prob- lem 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

ARCHITECTURE DIAGRAM



A. 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

III. Conclusion

Creating immutable ledgers is one of the main values of Blockchain. This behavior helps us to achieve a system in which all the processes are transparent and unchangeable. Our System automates the process of generating certificates and reduces the manual work needed for the verification of the same. Students are also at comparatively minimal 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 stored in the blockchain while the original document will be in the Inter Planetary File System (IPFS). This will help us preserve the data and create transparency.

Drawbacks of existing system

- the certificates and marks cards are stored in our university 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 interviewer should waste his time on validating the given certificates is proper or not.

Acknowledgment

The author would like to thank our guide ***Prof.PARKAVI B*** for the constant support and encouragement they gave us. We are very thankful for all the faith they had in us. And finally, our friends and family for their support. The dedication of our team members and enthusiasm helped us to move forward.

Appendix A

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.