iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 10 **Issue:** VII **Month of publication:** July 2022

DOI: https://doi.org/10.22214/ijraset.2022.45246

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue VII July 2022- Available at www.ijraset.com

CertiSafe: A Blockchain Based Certificate Validation and Safety System

Sri Samanthula Bhuvaneswari[1], Rakhi Kumari[2], Ch. Pavangeethanjali[3]
[1, 2, 3]*Department of Computer Science and Engineering, Sridevi Women's Engineering College (India)*

Abstract: ***In every career progression, we receive certificates of degrees and achievements. In the recent times as the technology advances, we also have people cheating by forging and duplicating certificates. We see people duplicating certificates by forging their names on the genuine certificates. As mostly institutions have digitalised the paper certificates and now by adding this system at the issuing and receiving party can make the entire process safe and reliable. This paper proposes a system where the issuing party of the certificate can use this system to safeguard the certificates from duplication and the third party or receiving party can reupload and check if the certificate is genuine and not tampered.***
Keywords: Blockchain, Certificate validation, Digital signature, Hashing, Security

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.

II. LITERATURE REVIEW

Under literature review, the work contributed towards developing a blockchain system to verify the certificates is mentioned. We studied about the different features and types of blockchain. Integration of Digital Certificate Blockchain and Overall Behavioural Analysis using QR and Smart Contract by Jin Chieo used the QR code and smart contract features to enable the process of validation but we will be using python libraries and work on proof of work. Smart contract technology is true new definition of conventional industry and business processes. Being embedded in blockchains, smart contracts enable the contractual terms of an agreement to be enforced automatically without the intervention of a trusted third party. As a result, smart contracts can cut down administration and save services costs, improve the efficiency of business processes and reduce the risks. Although smart contracts are promising to drive the new wave of innovation in business processes, there are a number of challenges to be tackled. Generating the e-certificates using Ethereum is also one of the approaches. A variety of approaches have been implemented to ensure security of the certificates and protecting it from tampering. The Main purpose of this study is to develop a theoretical framework for blockchain. Our aim is to identify the barriers and main drivers of digital innovation and explore the possibilities of applications of blockchain.

III.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.

©IJRASET: All Rights are Reserved

IV. 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.

V. APPROACH

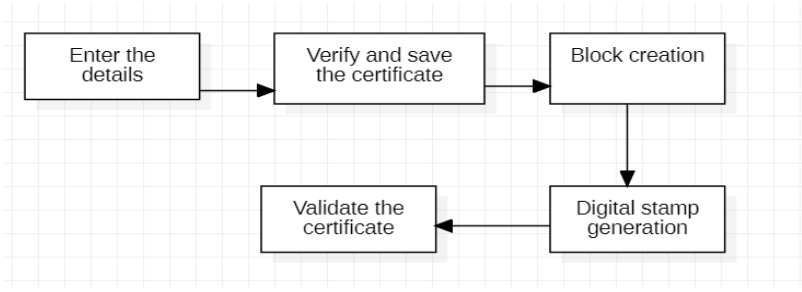
User Details of the certificate: In this module we create an interface to accept the user details such as roll number, student name and contact number.

*Save and verify the certificate :*In this module the user will upload the certificates. Before upload, those certificates are checked with the corresponding the institution and will be stored on the server.

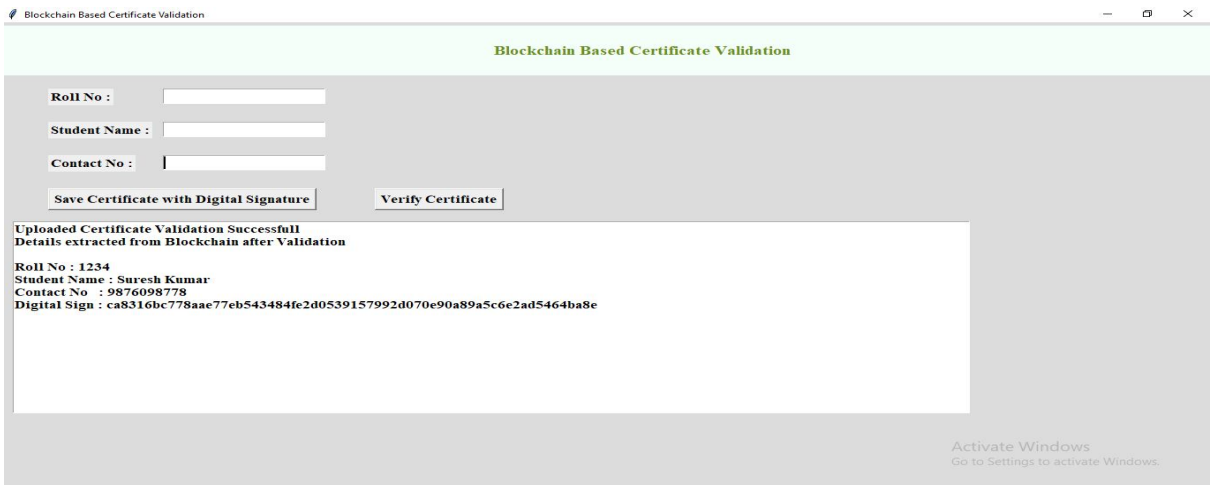
Block creation: A block is a container data structure. Here every certificate number will be created as a block. For every block a hash code will be generated for security.

Digital stamp generation: Now record will go to the party who authenticates digital signature and if the university is recognized then it will add its signature. And push this certificate to the blockchain (public repository) so that anyone can verify.

Validate the certificate: In this module verifier or companies or admin will take certificate from student and then upload to application and then application will convert certificate into digital signature and this digital signature will get checked/verified at Blockchain database and if matched found then Blockchain will retrieve all student details and display to verifier and if match not found then this certificate will be considered as fake or forge. Check the validity of the certificate based on hash value if it is valid stored in block else reject that certificate.



VI. RESULTS



VII. CONCLUSIONS

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.

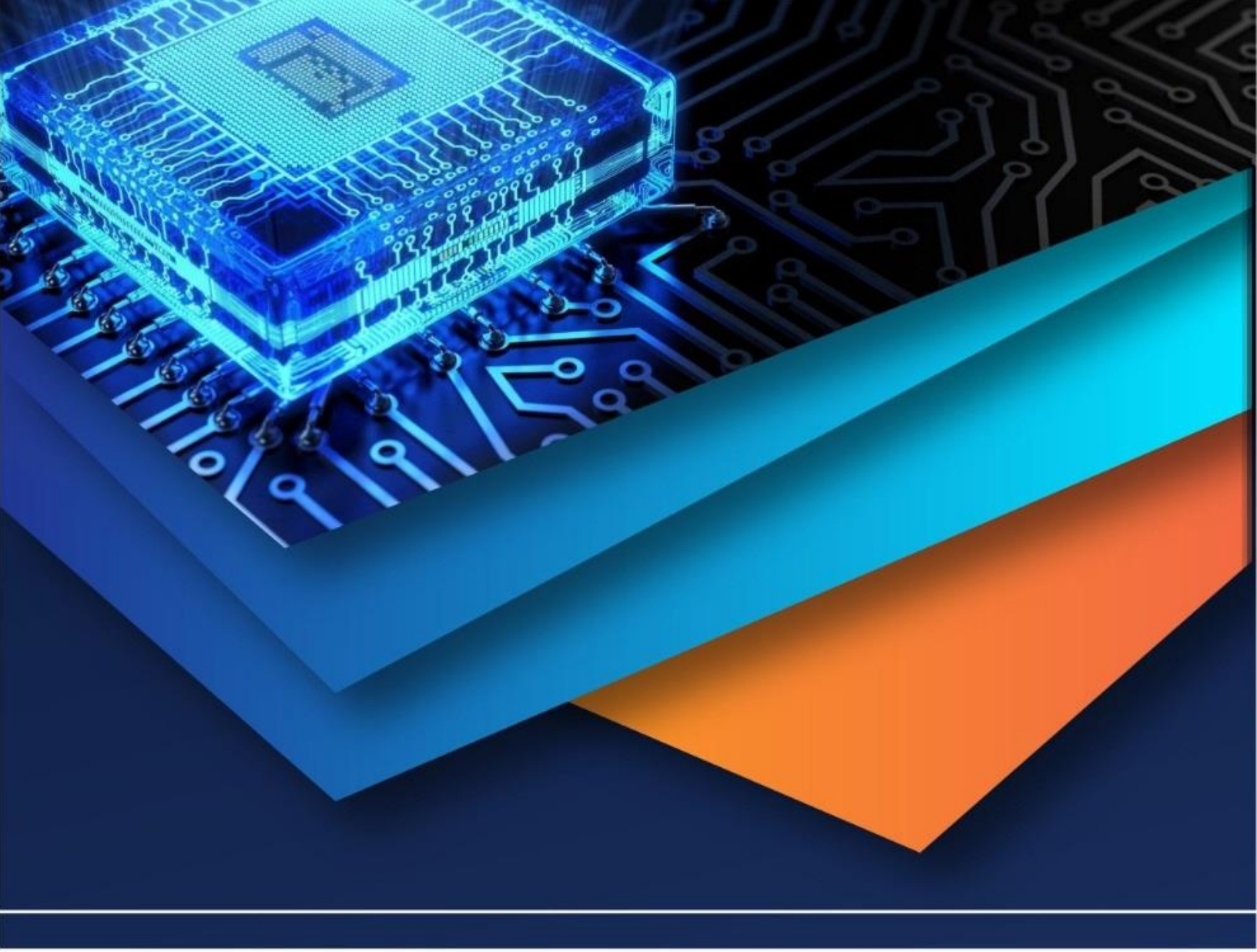
Future Scope: Students are also at comparatively low risk of losing the certificate. By using an additional hashing algorithm, we are decreasing the percentage of data being tampered with. The Hash of the certificate is being stored in the blockchain while the original document .This will help us preserve 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.

VIII. ACKNOWLEDGMENT

I would like to express my sincere gratitude to several individuals and organizations for supporting me throughout my study. I wish to express my sincere gratitude to my supervisor, and my friends for their enthusiasm, patience, insightful comments, helpful information, practical advice and unceasing ideas that have helped me tremendously at all times in my research and writing of this paper.

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
[6] Xiuping Lin, “Semi-centralized Blockchain Smart Contracts: Centralized Verification and Smart Computing under Chains in the Ethereum Blockchain”, Department of Information Engineering, National Taiwan University, Taiwan, R.O.C., 2017.
[7] Yong Shi, “Secure storage service of electronic ballot system based on block chain algorithm”, Department of Computer Science, Tsing Hua University, Taiwan, R.O.C., 2017.
[8] Zhenzhi Qiu, “Digital certificate for a painting based on blockchain technology”,Department of Information and Finance Management, National Taipei University of Technology, Taiwan, R.O.C.,2017.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)