Nanotechnology Perceptions
ISSN 1660-6795
www.nano-ntp.com

Certificate Verification And Validation Using Blockchain

K. Ragha Mani[1],Dr. B.Hari Krishna[2]

[1]PG Scholar, Department of Computer Science and Engineering , Malla Reddy Engineering College(A), Maisammaguda,Secunderabad-500100, District -medchal, Telangana,India.
[2]Associate Professor, Department of Computer Science and Engineering ,Malla Reddy Engineering ,College(A), Maisammaguda,Secunderabad-500100, District -medchal, Telangana,India.
Email: [1]kraghamani9999@gmail.com,[2]harikrishna@mrec.ac.in

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 .

Keywords: Blockchain, Digital Certificate, Hashing, Validation.

I .INTRODUCTION

Blockchain was introduced in the year 2008 by Satoshi Nakamoto. Blockchain is one of the online ledgers which provide decentralized and transparent data sharing. In this project, we design an android application used to provide secure verification of our certificates. In nowadays, all Graduation certificates and transcripts hold information that is easily tampered illegally by individuals and should not be easily accessible to outside entities. Hence, there is a high need for an efficient mechanism, that can guarantee the information in such certificates is original, which means the document has originated from a reliable and authorized source and is not forged. Various systems have been designed to secure e-certificates for education institutions and to store them securely in cloud-based systems

II.RELATED WORK :

In our application the first page is admin login, the next page consists of add student and certificate and last verifier page. The admin can log in to our application using the admin login id and password. Then the admin can add the student and their certificates by tap the add student and add certificate button. Next, the verifier can validate the certificate using the verifier login id and password. They provide the login id of the student and select the

certificate type and tap the verify button. If the uploaded certificates are original then the result will be a success. Otherwise, the result will be error and modified

S no	Authors	Title	Conference/journal	Year
1	Nitin Kumavat, Swapnil Mengade, Dishant Desai, Jesal Varolia	Certificate Verification System using Blockchain	Computer Engineering Department, Mumbai university	2024
2	Omars Saleh, Osman Ghazali, Muhammad Ehsan Rana	Blockchain Based Framework for Educational Certificates Verification	Studies, Planning and Follow-up Directorate, Ministry of Higher Education	2020
3	S. Sunitha Kumari, D. Saveetha	Blockchain and Smart Contract for Digital Document Verification	Studies, Planning and Follow-up Directorate, Ministry of Higher Education	2018
4	D. S. V. Madala, M. P. Jhanwar, A. Chattopadhyay	Certificate Transparency Using Blockchain	IEEE International Conference on Data MiningWorkshops	2018
5	Marco Baldi, Franco Chiaraluce, Emanuele Frontoni, Giuseppe Gottardi, Daniele Sciarroni, Luca Spalazzi	Certificate Validation through Public Ledgers and Blockchains	Proceedings of the First Italian Conference on Cybersecurity	2017

PROPOSED MODEL :

In this proposed system the academic, sports certificates are converted into digital certificates using sampling and quantization. Then the certificates are added with the hash values generated for the digital certificate and store it into the blocks. The chaotic 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.

For the purpose of certificate verification, once a certificate is issued and converted to a digital format, a hash is generated for the certificate, which is then stored in the blockchain. This ensures that any attempt to alter the certificate can be immediately detected because the hash value will no longer match the one stored in the 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.

III.SYSTEM ARCHITECTURE:

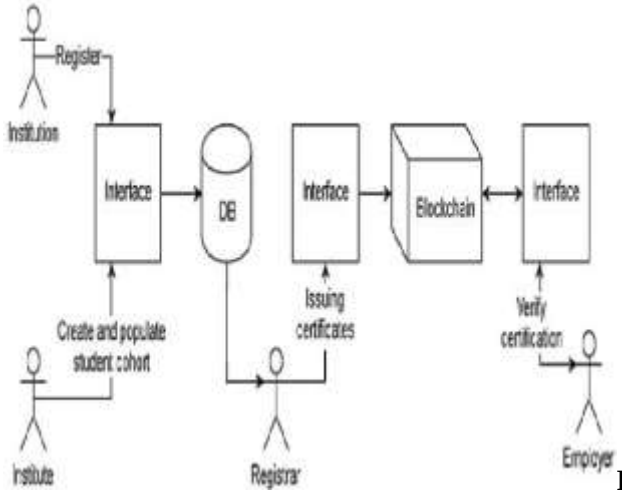

Figure.1.System Architecture

IV.METHODOLOGY

Existing system challenges

The current system of certificate management involves manually verifying certificates, which is time-consuming and prone to errors. Admins log into systems, add certificates, and verifiers manually authenticate these certificates. However, this centralized approach suffers from issues such as data manipulation, high maintenance costs, and limited scalability.

1.Proposed Blockchain-based System

The proposed system employs blockchain technology to digitize and store certificates, adding an extra layer of security through cryptographic hashing. A chaotic algorithm

generates a unique hash for each certificate, which is then stored in a blockchain block. This system consists of three main components:

Admin Interface: Admins register students, upload their certificates, and store them in the blockchain.

Verifier Interface: Employers or educational institutions can verify the authenticity of certificates by querying the blockchain using a mobile application.

Blockchain: The decentralized ledger that holds all certificates and ensures their immutability and verifiability.

2.Chaotic Algorithm for Hash Generation

The chaotic algorithm is used to generate the hash values for certificates. These algorithms are effective for cryptographic purposes because of their sensitivity to initial conditions and their ability to produce random-like, yet deterministic, outcomes. Once the hash value is generated for a certificate, it is stored in the blockchain alongside a timestamp and the previous block's hash, ensuring that the certificate's authenticity can be verified over time.

3.Process Flow

The process begins when a student receives a digital version of their certificate from an educational institution. The certificate is then processed using the chaotic algorithm to generate a hash value. This hash value is stored in the blockchain, forming a secure and immutable record. When the student applies for a job or further education, they can provide a QR code linked to their blockchain-stored certificate. The verifier scans the QR code and checks the blockchain for the corresponding hash value. If the values match, the certificate is confirmed as authentic; otherwise, it is flagged as invalid.

Advantages of Blockchain for Certificate Verification

•Security: Blockchain technology ensures that once data (i.e., the certificate) is entered into the ledger, it cannot be modified without consensus from the entire network, making the system highly resistant to tampering and fraud.

•Transparency: Every transaction or entry into the blockchain is transparent and can be verified by any party with the necessary permissions, ensuring accountability.

•Efficiency: The proposed system streamlines the verification process by eliminating the need for intermediaries. Verifiers can instantly check the validity of a certificate through a mobile app, reducing the time and cost associated with traditional methods.

•Decentralization: By distributing the certificate data across multiple nodes, the risk of a single point of failure is minimized, ensuring the system remains robust and reliable

Hashing Algorithms

Hashing plays a crucial role in creating a unique digital fingerprint (hash) for each certificate, which is stored on the blockchain. Common hashing algorithms used include:

SHA-256 (Secure Hash Algorithm-256):

- Most widely used in blockchain.
- Generates a fixed-length 256-bit hash regardless of the certificate's size.
- Any alteration to the certificate (even a single character) changes the hash drastically, ensuring tamper resistance.

SHA-3:

- An alternative to SHA-256, part of the Keccak family.
- Provides a higher level of security for systems requiring more resilience against future vulnerabilities.

Public-Private Key Cryptography

Blockchain systems rely on **asymmetric encryption** (public-private key cryptography) for both certificate issuance and validation:

Digital Signatures:

- When a certificate is issued, the issuer signs the hash of the certificate using their private key.
- Verifiers can use the issuer's public key to verify the signature and ensure the certificate's authenticity.

Elliptic Curve Digital Signature Algorithm (ECDSA):

Commonly used for digital signatures in blockchain due to its strong security and efficiency with smaller key sizes compared to RSA.

Helps verify the authenticity of certificates without exposing sensitive data.

Consensus Algorithms

To ensure certificates are securely added to the blockchain, consensus algorithms validate the transaction by achieving agreement among nodes. Popular consensus algorithms include:

Proof of Work (PoW):

Used in blockchains like Bitcoin.

Involves solving a computational puzzle to validate and add transactions (certificate data) to the blockchain.

Secure but energy-intensive and less efficient for certificate systems.

Proof of Stake (PoS):

More energy-efficient and scalable than PoW.

Validators are selected based on their stake (ownership) in the network.

Suitable for certificate verification blockchains as it provides security with reduced resource usage.

Practical Byzantine Fault Tolerance (PBFT):
Consensus algorithm designed for low-latency environments.

Suitable for permissioned blockchains often used in certificate verification, where trusted parties verify the certificates.

Smart Contracts

Smart contracts are self-executing contracts with the terms of an agreement directly written into code. They play a pivotal role in automating certificate issuance and validation on the blockchain.

Smart Contract Features:
Once a certificate is issued, the smart contract automatically stores the certificate data and hash on the blockchain.

For validation, users can query the smart contract by providing certificate details, which are checked against the blockchain record.

- Based on the hash match, the smart contract confirms whether the certificate is valid or tampered with.

Ethereum's Solidity Language:
- Most common for developing smart contracts.
- Facilitates automation of certificate issuance and real-time validation.

Merkle Trees

A **Merkle tree** is a data structure used in blockchain to efficiently verify large sets of data, such as multiple certificates.

Merkle Tree Structure:
Certificates are grouped, and their hashes are combined to form a tree of hashes.

The root of this tree (Merkle Root) is stored on the blockchain.

Individual certificates can be validated by comparing their hash with the Merkle Root, ensuring quick verification without requiring the entire dataset.

Permissioned vs. Permissionless Blockchains

Depending on the use case, the blockchain used for certificate verification can be either **permissionless** (public) or **permissioned** (private):

Permissioned Blockchain:
Common for academic institutions, corporations, or government entities.

Only authorized entities (e.g., universities) can issue and verify certificates.

Offers higher control and privacy for certificate management.

Permissionless Blockchain:
Open to anyone for certificate verification.

Provides transparency and immutability, making it suitable for public credential verification.

Interoperability Standards (DID & Verifiable Credentials)

Standards like **Decentralized Identifiers (DID)** and **Verifiable Credentials (VC)** are often used to make certificate verification more standardized across platforms:

DID (Decentralized Identifiers):
A unique identifier issued on the blockchain, allowing certificate holders to prove their identity without a centralized authority.

Allows certificate holders to own and manage their credentials.

Verifiable Credentials (VC):
Provides a standard data model for issuing, storing, and sharing credentials on the blockchain.Ensures interoperability across different systems and blockchains.

V.SCREEN SHOTS:
To run project double click on ‘run.bat’ file to start python server and get below output

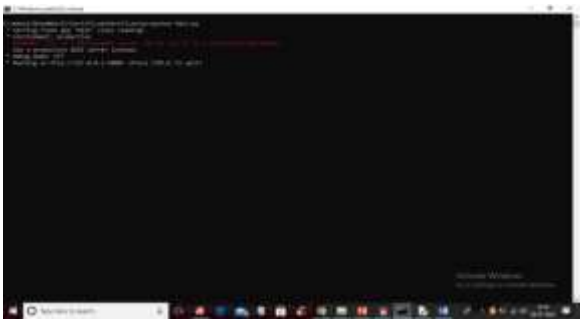

Figure.1) .bat file exe

In above screen python FLASK server started and now open browser and enter URL as http://127.0.0.1:5000/index and press enter key to get below page

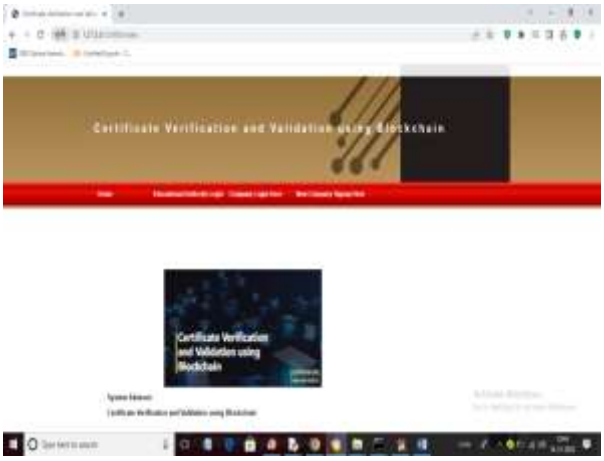

Figure.2) Home page

Figure.3) Admin Login page

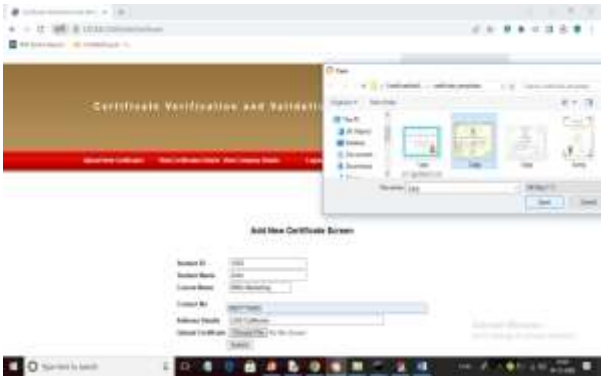

Figure.4)Upload page

Figure.5)Certificate Validation page

Figure.6)List of students with Qr code

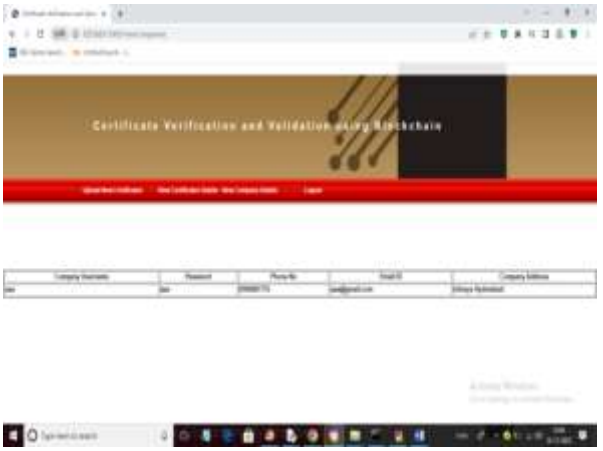

Figure.7)Details of a students

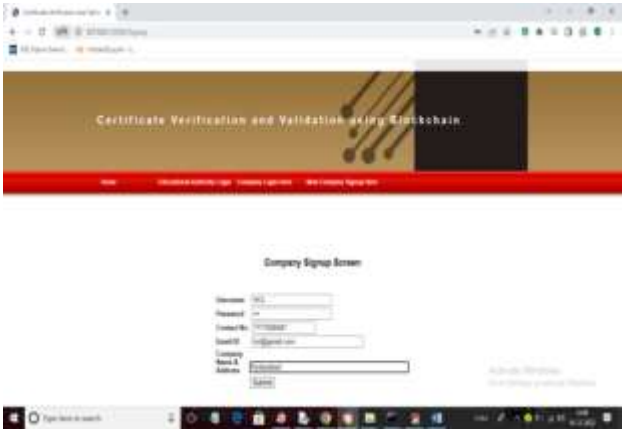

Figure.8) Company signup form

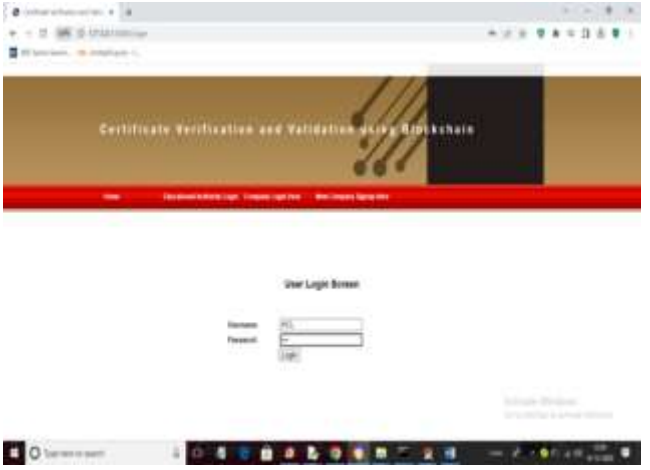

Figure.9) User login screen

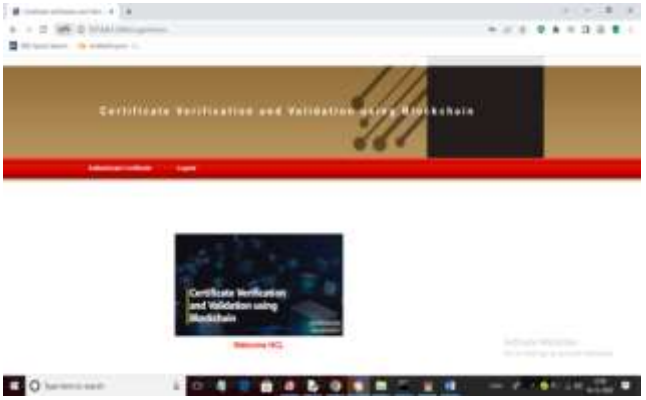

Figure.10)

Figure.11)Authenticate Certificate screen

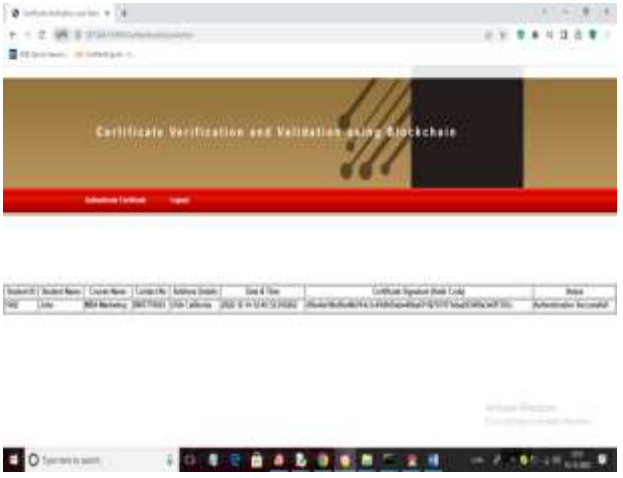

Figure.12)student authentication details

Figure.13)Authenticate upload screen

Now company or educational institution can validate certificate by scanning QR code and to do that, just double click on 'RunWebCam.bat' file to get below output

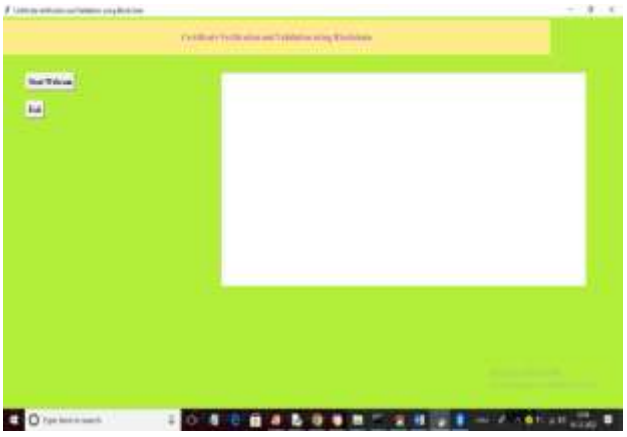

Figure.14) Home page

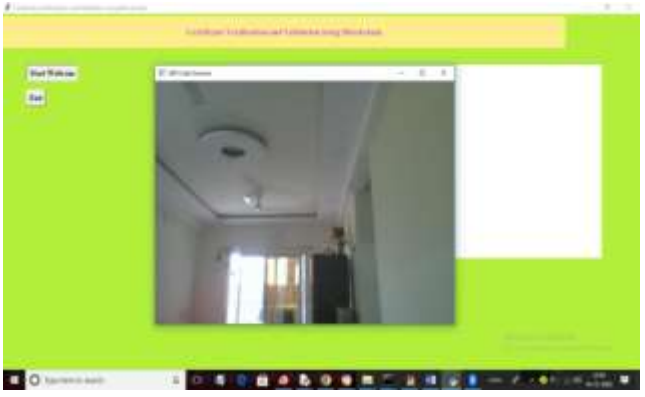

Figure.15)Web cam page

Figure.16)

In above screen once we show QR code then all details for that QR code certificate will be retrieve from Blockchain and display in above TEXT area. Similarly if we scan wrong CODE then will get below output

Figure.17)

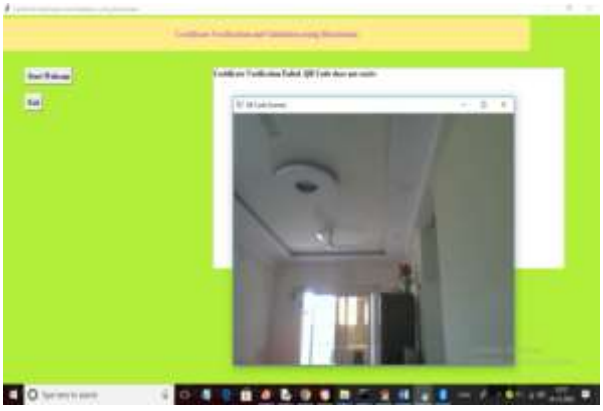

Figure.18)

VI CONCLUSION:

in this paper, we proposed a solution to the problem of certificate forgery based on blockchain technology. Providing security to the data is very important. By using the unchallengeable property of blockchain, we can provide more security for data and reduce the certificate forgery. The application can allow the user to view and validate the certificate. This system guarantees information accuracy and security and easy for people to manage digital certificates.

VII REFERENCES:

[1] Jiin-Chiou Cheng; Narn-Yih Lee; Chien Chi; Yi-Hua Chen, "Blockchain and Smart Contract for Digital Certificate" IEEE International Conference on Applied System Invention (ICASI),2018.

[2] Wang Z., Lin J., Cai Q., Wang Q., Jing J., Zha D. (2019) Blockchain-Based Certificate Transparency and Revocation Transparency. In: Zohar A. et al. (eds) Financial Cryptography and Data Security. FC 2018. Lecture Notes in Computer Science, vol 10958. Springer, Berlin, Heidelberg.

[3] D. S. V. Madala, M. P. Jhanwar, and A. Chattopadhyay, "Certificate Transparency Using Blockchain," 2018 IEEE International Conference on Data Mining Workshops (ICDMW), Singapore, Singapore, 2018, pp. 71-80, doi: 10.1109/ICDMW.2018.00018.

[4] Aisong Zhang and Xinxin Ma, "Decentralized Digital Certificate Revocation System Based on Blockchain

[5] Marco Baldi, Franco Chiaraluce, Emanuele Frontoni, Giuseppe Gottardi, Daniele Sciarroni, and Luca Spalazzi "Certificate Validation through Public Ledgers and Blockchains In Proceedings of the First Italian Conference on Cybersecurity.

[6] Nitin Kumavat, Swapnil Mengade, Dishant Desai, JesalVarolia, " Certificate Verification System using Blockchain" Computer Engineering Department, Mumbai University.

[7] S.Sunitha kumari, D.Saveetha "Blockchain and Smart Contract for Digital Document Verification" Department of Information Technology- SRM Institute of Science and Technology.

[8] Omars Saleh, osman ghazali, muhammad ehsan rana, "Blockchain based framework for educational certificates verification" Studies, Planning and Follow-up Directorate, Ministry of Higher Education and Scientific Research, Baghdad, Iraq. School of Computing, University Utara Malaysia, Kedah, Malaysia.