

VERIFICATION OF CERTIFICATES USING BLOCKCHAIN

K. Srinivas Rao, Associate Professor, Department of Electronics and Communication Engineering,
Kallam Harinadha Reddy Institute of Technology, Guntur, India

M. LSV Subrahmanyam, R. RVV Sai, J. Pavan Kumar, K. Balaji, K. Vamsi Student, Department of Electronics and
Communication Engineering, Kallam Harinadha Reddy Institute of Technology, Guntur, India

ABSTRACT:

In this project to secure academic certificate and for accurate management and to avoid forge certificate we are converting all certificates into digital signatures and this digital signature will be stored in Blockchain server as this Blockchain server support tamper proof data storage and nobody can hack or alter its data and if by a chance if its data alter then verification get failed at next block storage and user may get intimation about data alter. In Blockchain each data will be stored by verifying old hash codes and if old hash codes remain unchanged then data will be considering 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.

Key words: Block chain, Hyperledger, digital certificate, hashing.

1. INTRODUCTION

According to, educational certificates are extremely reputable as they function as associate indicators of the human capital of their bearers. Human capital refers to the abilities, competencies, information, and aptitudes achieved through education. educational qualifications are significantly vital working things as they function as a guarantee of not simply the information, experience, and skills of the holders however additionally of their talents, responsibility, and dedication. From the attitude of the bearers, found a correlation between academic attainment levels and higher employment prospects, and economic security. recognized that educational qualifications are deemed to be real after they are presented by a university genuine when they are approved to award such certificates. Because they are thus valuable, people often lie about their academic qualifications by producing fake certificates. mentioned that within us there are presently a pair of million faux degree certificates in circulation and three hundred unauthorized universities operational. indicated that the United States has a very large number of fake institution establishments within the world followed by the UK that has concerning 270 fake institutes. Healy (2015) found that up to thirty-fifth of candidates in Australia falsified their educational credentials for the sake of employment. discovered that

almost all candidates lie a minimum of concerning some a part of their academic credentials and skill. mentioned that educational certificate fraud prices employers concerning \$ 600 billion per annum. To overcome this, we tend to mistreatment we are using technology known as Blockchain. Blockchain is that the backbone Technology of the Digital Crypto Currency Bitcoin. The blockchain could be a distributed info of records of all transactions or digital events that are dead and shared among taking part parties. every group action is verified by the bulk of participants of the system. It contains every single record of every group action. Bitcoin is that the hottest cryptocurrency associate example of the blockchain. Blockchain Technology initial came to light-weight once someone or a cluster of people name 'Satoshi Nakamoto' revealed a report on "Bitcoin: A peer to look electronic money system" in 2008. Blockchain Technology Records group action in Digital Ledger that is distributed over the Network so creating it incorrupt. something important like Land Assets, Cars, etc. is recorded on Blockchain as a group activity.

1.1 Building trust with Blockchain:

Blockchain enhances trust across a business network. It's not that you just can't trust those with who you conduct business with it's that you just don't got to once in operation on a Blockchain network. Blockchain builds trust through the subsequent for the attributes for this purpose.

- **Distributed:** The distributed ledger is shared and updated with each incoming group action among the nodes connected to the Blockchain. All this can be worn out real time as there's no central server dominant the information.
- **Secure:** there's no unauthorized access to Blockchain created attainable through Permissions and Cryptography.
- **Transparent:** as a result of each node or participant in Blockchain contains a copy of the Blockchain information, they need access to all or any group action information. They themselves will verify the identities while not the requirement for mediators.
- **Consensus-based:** All relevant network participants should agree that a group action is valid. this can be achieved through the utilization of agreement algorithms.
- **Flexible:** good Contracts that are dead supported bound conditions may be written into the platform. Blockchain

networks will evolve in pace with business processes and also for the future

1.2 Benefits of Blockchain Technology:

- **Time-saving:** No central Authority verification is required for settlements creating the method quicker and cheaper.
- **Cost-saving:** A Blockchain network reduces expenses in many ways in which. No would like for third-party verification. Participants will share assets directly. Intermediaries are reduced. group action efforts are reduced as each participant contains a copy of the shared ledger.

1.3 Problem Statement:

Finding the right candidate for the job when hiring has been a difficult work for employers or HRs of a company. One of the significant issues is the fake credentials given by the candidate like certificates. According to the survey of HireRight, about 56% of the educational credentials provided for background verification had discrepancies. Due to this, an eligible candidate may lose his opportunity to an ineligible candidate.

1.4 Objective:

To define a general schema and use cryptographic methods to create Digital Academic Certificates or to build a secure, scalable blockchain-based storage system for storage of the digital certificates. or to develop an interface for data custodian and data consumer to store, manage, and deploy data certificates and upload, Authenticate certificates respectively.

1.5 Description:

The physical certificates are converted into digital records. These digital records are stored in a blockchain network. Where the records once stored are immutable and cannot be changed forever due to the smart contracts. These digital records are created by the institution (issuer) and are deployed on the blockchain. A Certificate Id is sent to the user that is student or holder of the certificate. This Id can be sent to anyone intended to check or authenticate the digital certificate. For example, A company that is hiring the candidate and needs to verify the certificate authenticity of the candidate can verify it through our web application which is developed using MongoDB, React.JS.

2. LITERATURE SURVEY:

[1] Zibin Zheng et al.

Blockchain as a Notarization Service for information Sharing with Personal data Store: Provides a blockchain-based design to produce the credibility verification of the shared documents in period whereas maintaining necessary privacy. Discusses usage of blockchain to realize Associate in Nursing audit path of

the accesses to the shared data. Whereas keeping the audit path non-public to the people involved.

[2] Richard Nuetey et al.

Block-certs and therefore the Digital Certificates project was undertaken at Media Labs Massachusetts Institute of Technology: An incubation project by the Media research laboratory Learning Initiative. Associate in Nursing the Learning Machine that builds a scheme for making, sharing, and validating bitcoin blockchain-based academic certificates. Digital certificates square measure registered on the Bitcoin blockchain, cryptographically signed, and tamper proof.

[3] Omar S Saleh et al.

Authentication of User Details: The blockchain should certify users. during this case, the users square measure students, universities, institutes, employers, etc. every user in an exceedingly blockchain ledger are verified for accessing the certificate kept thereon. Authentication for users is thru a username and secret, or some system can even have multiple authentication systems like biometric, etc. as an example, the leader required to verify the certificate should initial be part of the blockchain and therefore the recipient can authorize the leader to look at the certificate and verify it.

[4] A Gayatri et al.

Cheng university 'Blockchain and good Contract for Digital Certificate: Jin-chiou developed a software package so as to avoid counterfeiting certificates. thanks to the dearth of Associate in Nursing anti-forge mechanism, the graduation certificate is to be solid. so, the decentralized application was designed to support Ethereum blockchain technology. First, generate the digital certificate for the paper certificate then hash worth created for the certificate is kept within the blockchain system. Even it wants to verify the credibility of the certificate it needed another scanning app to scan the certificate. The system saves on paper, stops document forgery. however, the QRCode should be scanned with a smartphone and an online association is needed.

[5] A Gayatri et al.

Project done by Ze Wang et al: Ze Wang et al designed blockchain-based certificate transparency and revocation transparency system. during this system, the certificate authority (CA) signed the certificate, and therefore the revocation standing data of the revered certificates square measure revealed by the topic (Certificate Authority). Public logs square measure want to monitor the CAs operation. this method was enforced with Firefox and nogix. this method provided the trust however Certificate validation is delayed and a false sense of security.

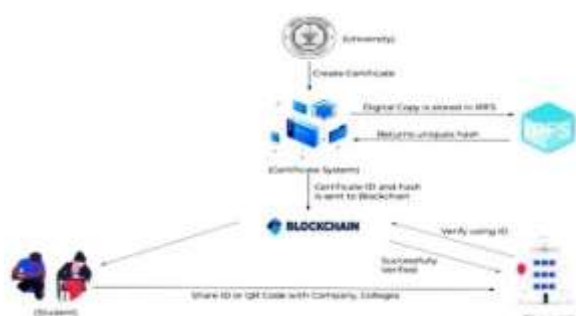
3. METHODOLOGY

- A digital certificate is essentially a JSON Object with the necessary fields needed for our cert-issuer code to place it

on the blockchain. For which a hash can be generated and used for verification purposes.

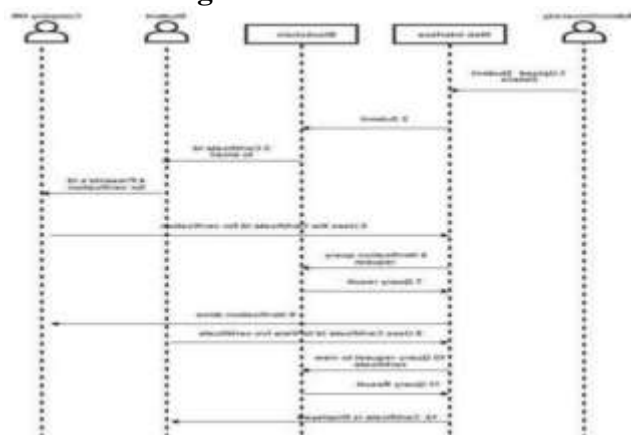
- Blockchain storage methodology Ethereum is utilized to develop an architecture to store and manage digital certificates.
- Modern web development technologies such as React-js, Node-js are utilized to build an interface that facilitates the user to view, manage, and verify documents online.

3.1 ARCHITECTURE DIAGRAM



A model may be a complete, basic, and simplified description, of software system design that consists of multiple views from a selected perspective or view point as shown in above figure. A read maybe an illusion of a complete system from the attitude of a connected issues. It's accustomed to describe the system from the point of view of various stakeholders like end-users, developers, project managers, and testers. Here Blockchain is the common medium of technology going to be used in the security of the data. So, we can solve the problem of counterfeit certificates.

3.2 Workflow Diagram:



Step 1: University will fill student academic details in a form provided using Dapp interface.

Step 2: University submits the pre-viewed form details to Blockchain.

Step 3: When the certificate is uploaded into Blockchain. Certificate hash code is generated and sent to respective student.

Step 4: Students can share the Certificate hash code for certificate verification.

Step 5: With the help of hash code Company HR can verify the certificate.

Step 6: Verification of Certificate hash code query request will take place.

Step 7: Query result is displayed i.e., verified or failed.

Step 8: HR can confirm the certificate.

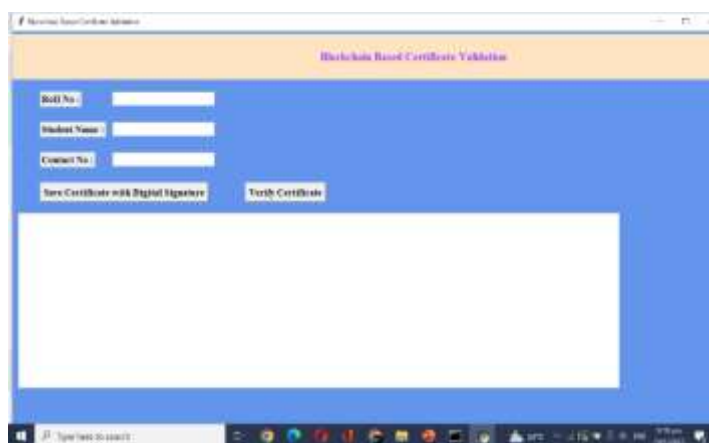
Step 9: The student will use his Certificate hash code to view the certificate.

Step 10: Query request to search Certificate hash code in the blockchain.

Step 11: Query result for the Certificate hash code will be displayed.

Step 12: Students can view their Certificate (Verification of certificate is optional for student).

OUTPUT SCREEN:



4.APPLICATIONS

- Certificates are securely stored on Blockchain Network.
- Right person will get the Right Job Opportunity.
- Issues related to fake certificates will be avoided.
- Every time student needs to attest his/her certificate for the verification. This can be avoided.
- Certificates are easily accessible.
- Once the certificates are deployed on the Blockchain Network that will become Immutable. So, Certificate Data will not be altered.
- Manual Verification of the Certificate takes more time. This issue will be solved using Digital Certificate Verification System That will

take very less time to verify Certificate.

5.ADVANTAGES

1. In Blockchain packages, Learning short time i.e., High execution speed,
2. Comparison of certificates are fast i.e., High flexible.
3. It has low memory requirements
4. Secure Server
5. As we have seen earlier, Python can be extended to other languages. You can write some of your code in languages like C++ or C. This comes in handy, especially in projects.
6. Since Python forms the basis of new platforms like Raspberry Pi, it finds the future bright for the Internet of Things. This is a way to connect the language with the real world.

6.CONCLUSION

The proposed system works well on the involvement of multiple companies and institutions for the uploading of the certification details. This system plays a safer role in guarding the data secure with the help of the discussed technology. Overcomes the issues discussed above. The conversion of data into hash values play a major role in security and the interconnection of those hash values through blockchain makes it even stronger in security. The validator can be of any party, either an educational institution or a company sector. Any of the interested sectors could possibly check the received certificates for the genuinely. The certificate uploaders would need the permission and access from the smart contract owner to upload the details. The smart owner checks the requested client for they are a proper certificate issuer. After validating the certificate issuer, a unique ID and Password helps them to upload the certification details. The updation of any existing certificates would lead to notify all the other certificate issuers in the node. Thus, it is in a highly safer hand.

7.REFERENCES

- [1] Tengyu Yu, Blockchain operation principle analysis: 5 key technologies, iThome, <https://www.ithome.com.tw/news/105374>
- [2] Jingyuan Gao, The rise of virtual currencies! Bitcoin takes the lead, and the other 4 kinds can't be missed. Digital Age, <https://www.bnext.com.tw/article/47456/bitcoin-ether-li-tecoin-ripple-differences-between-cryptocurrencies>
- [3] Smart contracts whitepaper, <https://github.com/OSELab/learning-blockchain/blob/master/ethereum/smart-contracts.md>
- [4] Gong Chen, Development and Application of Smart Contracts, <https://www.fisc.com.tw/Upload/b0499306-1905-4531-888a-2bc4c1ddb391/TC/9005.pdf>
- [5] Weiwei He, Exempted from cumbersome auditing and issuance procedures, several national junior diplomas will debut next year. iThome, <https://www.ithome.com.tw/news/119252>
- [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.
- [9] Weiwen Yang, Global blockchain development status and trends, <http://nmarlt.pixnet.net/blog/post/>
- [10] Benyuan He, "An Empirical Study of Online Shopping Using Blockchain Technology", Department of Distribution Management, Takming University of Science and Technology, Taiwan, R.O.C., 2017.
- [11] Chris Dannen, Introducing Ethereum and Solidity, <https://www.apress.com/br/book/9781484225349>
- [12] Jan Xie, Serpent GitHub, <https://github.com/ethereum/wiki/wiki/>