Blockchain Based Digital Certificate Generation and Verification System

Sanjay Janyani[#1], Latika Gurnani[#2], Jiten Tolani[#3], Pooja Shetty[#4]

[#1,2,3]*Student, Department of Information Technology, Vivekanand Education Society's Institute of Technology Mumbai 400074, India.*

[#4]*Assistant Professor, Department of Information Technology, Vivekanand Education Society's Institute of Technology Mumbai 400074, India.*

[1]2016.sanjay.janyani@ves.ac.in

[2]2016.latika.gurnani@ves.ac.in

[3]2016.jiten.tolani@ves.ac.in

[4]pooja.shetty@ves.ac.in

***Abstract*— Each year millions of students graduate. A large number of students apply for higher studies and interview posts where they need to submit their mark sheets and other certificates. The issuer (graduate institute) goes through a laborious task generally manually, to maintain and share. And also verify the certificates to the applying organization if at all. Currently there is no proper system of verifying the certificates from the graduate institute. Also, academic institutes have been having a long-standing issue with counterfeit of certificates. This issue can be addressed by creating Digital Certificates or E-Certificates. Digital certificates can be generated using the blockchain technology with QR-code embedded on each certificate. To address the verification problem, the verifier would have to just scan the QR- code and validate it. This concept will help educational institutions and other service sectors like healthcare, bank to verify certificates of a particular individual in very less time, effortlessly and in a cost-effective manner.**

***Keywords*— BlockChain, Digital Certificate, QR code, Verification, Ethereum.**

I. INTRODUCTION

A. Background Information

Blockchain has emerged as one of the promising technologies and has been growing rapidly, with its applications on a wide range of domains. A blockchain, is a growing chain of records called blocks, that are linked and secured using cryptography [2]. Each block contains data, a cryptographic hash of the previous block providing a secure linkage between blocks, a timestamp to validate etc. It is a decentralised system where the data is distributed among various participants referred to as Nodes. Every node has a consistent copy of data. Consequently, the nodes maintain the database together. A new block becomes validated only once it has been verified by multiple parties which are binded by a set of rules called Smart Contracts, making addition of new blocks secure and structured. Smart contracts are a set of rules that run on blockchain in a form of a computer program [1]. Furthermore, making modification to data arbitrarily very difficult.

B. Rationale

The students graduating either choose to continue their studies or go hunting for jobs. In both the cases they are required to submit their certificates. A couple of times students find that they have lost the certificates and they need to reapply which is a long procedure and has to go through multiple verification taking a lot of time. Also considering increase in forgery of documents, the organization to which the certificates are submitted find it difficult to verify the certificates [5]. There is no effective way to check for the forgery.

C. Objectives

To address the issue of distribution and verification of certificates we propose a decentralized application that does Digital Certificate Generation and Certificate Verification module. An effective solution by integrating the concept of Blockchain and QR code has been proposed. The system saves paper, cuts management costs, prevents forgery, and provides accurate and reliable information of certificates.

II. LITERATURE SURVEY

Blockchain technology has a wide range of applications and its own challenges. The comprehensive overview on blockchain technology with blockchain architecture provided by P. Tasatanattakool and C. Techapanupreeda [6] and the key characteristics of blockchain by Z. Zheng, et al [9] inspired us to adapt Blockchain for application development. Smart contract technology is reshaping conventional industry [10]. One of the most important features of blockchain is the security it can provide for the data [8]. Hence, we use blockchain for verification of stored data and document forgery can be reduced.

Various technologies have been suggested to reduce the incidence of certificate forgeries and ensure the security, validity and confidentiality of graduation certificates. Using digital signatures in e-documents makes it vulnerable to security flaws as it uses key for any modification in the document. Among the various methods discussed we find the blockchain-based system the most efficient way to reduce the certificate forgery [5]. As Blockchain is a decentralized system in which each node saves and verifies the same data. So, with this system the likelihood of forgery is almost none. Anyone in the system can see the process of request and grant of the certificates making it completely transparent. Companies or organizations can thus inquire for information on any certificate from the system [2].

Sankara Narayanan gives an overview of the working of QR-code and its implementation [7]. In QR-Code data is encoded in both the vertical and horizontal direction, thus holding up to a few hundred times more information than a traditional bar code. QR Code holds a considerably greater volume of information than a bar code. Hence QR Code seems an ideal option for verification and easy access of certificates. Further Ahamed, et in their paper discuss about the two security models: validation model to securely transfer confidential data using RSA cryptography and verification model to verify information using RSA digital signature mechanism [3]. These concepts can be used to introduce certain security solutions such as use of short domain names, including signage etc. that need to be taken care while implementing the QR-Code.

III. System Implementation

A. *Overview*

The issuer needs to first submit all the credentials of every student. These credentials need to be verified by all the concerned authorities. After the verification is done a certificate is generated with a unique QR code embedded on it. This E-certificate is mailed to the student. Students can use this certificate for company's or wherever it is needed. The company can verify the originality of the certificate by scanning the QR code on the certificate.

B. *Methodology*

The system has four stakeholders:

- Certificate Issuers
- Two Higher Authorities
- Students

1) Certificate Issuers: The student authority or the event authority is responsible for uploading the students details for the generation of certificates either by entering each student details individually or bulk upload by uploading the excel sheet containing student details.

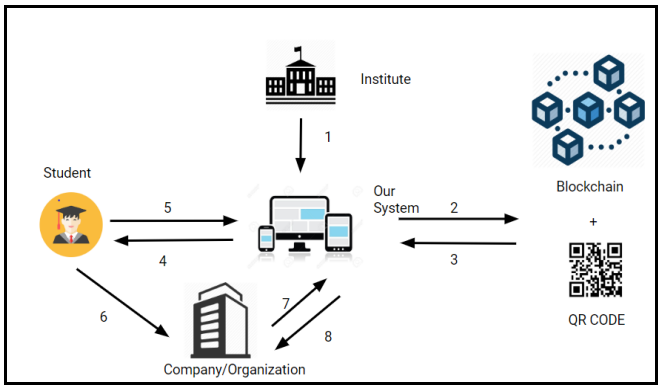

Fig. 1. Modular Diagram of proposed system

2) Higher Authorities: There are two higher Authorities which are responsible for verifying the certificate details and then approving them for the issue of certificates. Once both the authorities verify the details the certificates with QR code embedded on each certificate are generated.

3) Students: Once the certificates are generated the certificate links are sent to each student whose certificate is generated. The student can open the link and then download the soft copy of the certificate and can use this link or the ecopy for sharing the certificates to further companies or Schools

Process:

1) Firstly, the issuer needs to grant the certificates of the student by entering all the credentials of the student. The issuer can select from a set of available certificate templates. This data is then stored in the Blockchain.

2) Next the higher authorities need to verify the certificate.

3) Instead of distributing the hard copies of each certificate our system automatically sends email to every student with embedded unique QR code on each and every certificate.

4) Student can login in into our portal and download the copy of E-certificate which is available 24*7

5) Students can use this E-certificate or unique link (URL) of certificate to apply for various companies or wherever it is needed.

6) Once the company receives the certificate of students, they can verify the certificate by submitting the link of the certificate or just scanning the unique QR-code of the certificate.

7) Our system verifies whether it is the legitimate certificate or not. Based on which it sends the response to the company that whether the student actually owns the certificate or not.

C. Operation

1) Certificate Generation

After certification issuers have entered the information of a graduate, the system generates an e-certificate containing a QR code after few verifications. The data of each certificate is then recorded in the blockchain. Next, the system sends a notification and e-certificate link to the graduate for future inquiries. The process has been shown in Figure 2.

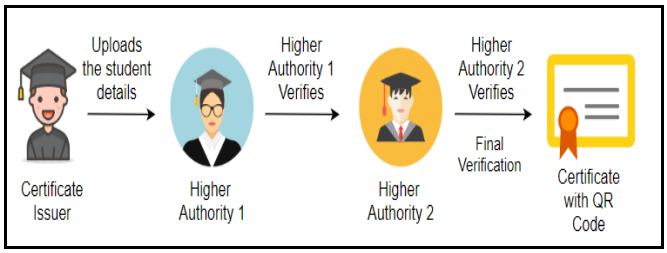

Fig. 2. Flow Diagram of Certification Generation

Fig. 3. E-certificate generated

2) Verification by Companies or Organisations

When a company acquires an e-certificate link or soft copy of the certificate from a job applicant, they can verify the veracity of the associated certificate either by scanning the QR code or by using the link provided by the job applicant. The message "Valid Certificate" is displayed only when the information from applicants matches the information in the system.

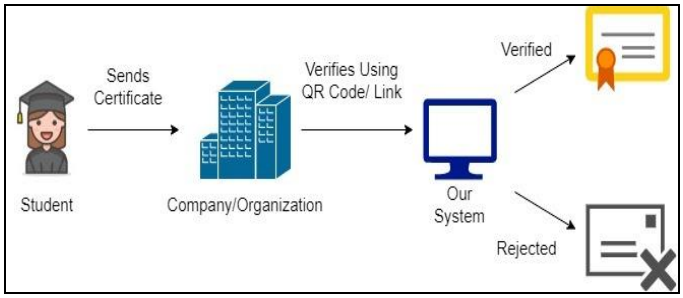

Fig. 4. Flow Diagram of Verification of Certificates

IV. Conclusion

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. The proposed new blockchain-based approach would reduce the certificate forgery to a large extent. Organizations can thus get information about any certificate at any time from the system. Added to saving on paper, cuts management costs. Also, this system assures information accuracy and security.

V. Future Scope

To further enhance the proposed solution, the system could be scaled up to university level and digitize the entire process of verification and authentication of documents. The solution can be customized for a company or institute.

REFERENCES

[1] B. K. Mohanta, S. S. Panda and D. Jena, "An Overview of Smart Contract and Use Cases in Blockchain Technology," 2018 9th International Conference on Computing, Communication and Networking Technologies (ICCCNT), Bangalore, 2018, pp. 1-4.

[2] Jiin-Chiou Cheng, Narn-Yih Lee, Chien Chi, and Yi-Hua Chen, "Blockchain and Smart Contract for Digital Certificate" Proceedings of IEEE International Conference on Applied System Innovation 2017

[3] M. S. Ahamed and H. Asiful Mustafa, "A Secure QR Code System for Sharing Personal Confidential Information," 2019 International Conference on Computer, Communication, Chemical, Materials and Electronic Engineering (IC4ME2), Rajshahi, Bangladesh, 2019, pp. 1-4.

[4] Murat Yasin Kubilay, Mehmet Sabir Kiraz, Hacı Ali Mantar, "CertLedger: A new PKI model with Certificate Transparency based on blockchain," in Computers & Security, vol 85, August 2019.

[5] Neetu Gopal, Vani V Prakash, "Survey on Blockchain Based Digital Certificate System," in International Research Journal of Engineering and Technology (IRJET), vol 5, issue 11, Nov. 2018.

[6] P. Tasatanattakool and C. Techapanupreeda, "Blockchain: Challenges and applications," 2018 International Conference on Information Networking (ICOIN), Chiang Mai, 2018, pp. 473-475.

[7] A Sankara Narayanan, "QR Codes and Security Solutions," in International Journal of Computer Science and Telecommunications (IJCST), vol3, issue 7, July 2012.

[8] S.Sunitha Kumari, D.Saveetha, "Blockchain and Smart Contract for Digital Document Verification," in International Journal of Engineering and Technology (IJET), vol.7, 2018.

[9] Z. Zheng, S. Xie, H. Dai, X. Chen and H. Wang, "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends," 2017 IEEE International Congress on Big Data (BigData Congress), Honolulu, HI, 2017, pp. 557-564.

[10] Zibin Zheng, Shaoan Xie, Hong-Ning Dai , Weili Chen, Xiangping Chen, Jian Weng ,Muhammad Imran, "An overview on smart contracts: Challenges, advances and platforms," in Future Generation Computer Systems, vol 105, April 2020.