IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol.-7, Issue-4, April 2019 E-ISSN: 2347-2693

E-Certificate Authentication System Using Blockchain

A.G. Said[1], R.P. Ashtaputre[2], B. Bisht[3], S.S. Bandal[4], P.N. Dhamale[5*]

[1,2,3,4,5]Dept. of Computer Engineering, All India Shri Shivaji Memorial Society's Institute of Information Technology, Savitribai Phule Pune University, Pune, India

Corresponding Author: 31payaldhamale@gmail.com

DOI: https://doi.org/10.26438/ijcse/v7i4.191195 | Available online at: www.ijcseonline.org

Accepted: 12/Apr/2019, Published: 30/Apr/2019

Abstract— The traditional system of using and maintaining paper certificates is now facing a threat of forging and modifying the data. This forging of data on the certificates has become a very easy task, which reduces the credibility of paper certificates. Thus, there is a need of an effective anti-forge mechanism to reduce the counterfeiting of certificates. An E-certificate generation and authentication system based on blockchain technology is so proposed. Blockchain provides incorruptible, unmodifiable and encrypted data features. Thus, by using blockchain, an E-certificate with features like anti-counterfeit, anti-forge and verifiability is generated. Students won't be able to forge the contents of E-certificates at all. The system, because of blockchain technology, will help to solve the problem of fraud certification by enhancing the credibility of the certificates. The system will also save the paper and management costs. Electronically, the loss risks of the certificates will be reduced. In short, the system is all beneficial to us. The working of the system in brief is: A valid electronic file of the certificate i.e. an E-certificate is generated on student's request. At the same time, that student's record is stored in the blocks of blockchain by making use of hash values. Along with E-certificate, a related QR code or unique serial number is also provided to the student. And then, the demand unit (e.g. company to which student applied for a job) can check the authenticity of the electronic file using the QR code or unique serial number which is based on the data stored in the blockchain.

Keywords—*E-Certificate,Blockchain,Cryptography,Anti-forge*

I. INTRODUCTION

A. Background

Blockchain is one of the most important and much needed advances in information technology. It has its main application in cryptocurrencies which is considered as a part of the industrial revolution. Bitcoin, being the most successful cryptocurrency until now has its safe and steady usage because of the underlying technology – Blockchain. Blockchain has become a hot topic for researchers, entrepreneurs, institutions and mainly to the countries. People are being aware of the potential of this technology which has its arms widespread. Blockchain is a distributed ledger which is used to store the distinct transactions in a secure, permanent and verifiable manner. Being a distributed ledger, blockchain can be used on P2P network. This is also known as decentralization property. Data is distributed among various nodes in the network and are so decentralized. P2P network adheres to communication among the nodes in the network and they collectively maintain the database. The transactions are stored in a chain of blocks linked to each other, thus name-Blockchain. Each block is created with a unique hash value using a hash function and timestamp. And the next block created knows the hash value of its previous block, which helps to connect the blocks with each other. Blockchain makes use of cryptography to store data in the blocks, that is the data is encrypted using cryptographic function and then it is stored in the blocks. This avoids any kind of mis-usage of data. The data stored in the blockchain is unmodifiable once it is validated by all the involved parties. If there is a need of alteration then the consensus needs to be taken and based on the majority of consensus it is decided whether the data can be altered or not. Although blockchain records are unalterable. Thus technically, blockchain technology has key characteristics of decentralization, unmodifiability, traceability and cryptography. Advantages of using this technology are reliability, trust, security, efficiency and many more.

B. Rationale

The advances in the information technology has made the data protection much needed than ever since. Data in learning context can be formal in case of students including their academic achievements and academic certificates and it can be informal which include information about researches, skills, online learning experience as well as individual interests. These data need to be safely stored and accessed in appropriate ways. Like the fraud certification of students or

the forging and counterfeiting of educational certificates is increasing nowadays and it needs to stop somewhere. Thus, the blockchain technology can be used due to its immutable property which will help in recording students' correct data. Plus being a reliable and trustworthy technology, the security and authority of data is assured. Thus, we are developing a certificate generation system based on blockchain. Also, there are often cases when students lose their educational and commendation certificates. Reapplying for hard copy is again a very time-consuming process. By contrast, an e-copy can save on paper as well as time and cost. Thus, we will be issuing an E-certificate to the applying student. The important work now is validating the certificate when students provide them to the companies for job interviews. Again, blockchain makes this task easier as the requesting user's ID is matched with data stored in blockchain and checked whether the certificate is actually granted or not.

C. Objective

We developed an E-certificate system based on blockchain which can be a decentralized application. By using the features of blockchain technology such as incorruptible, traceable and encrypted, the system works efficiently and reliably at each stage. The system avoids conventional paper certification methods which saves on paper. The management cost is also reduced. The system also prevents document forgery and provides correct information of students.

Section I of this paper gives introduction to the system, section II summarizes the related work on the system. Section III briefs about the system architecture and methodology. Section IV explains advantages of the system over previous systems. Section V discusses the results and outcome of the system. And, section V concludes the paper followed by acknowledgement and references.

II. RELATED WORK

[1] Lein Harn, Jian Ren, "Generalized Digital Certificate for User Authentication and Key Establishment for Secure Communications", 2011. The system provides the digital certificate platform by making use of a secret session key. It generates the key and uses it to authenticate the user.

[2] C. V. Malone, E. J. Barkie, B. L. Fletcher, N. Wei, A. Keren, A. Wyskida, "Mobile Optimized Digital Identity (MODI): A framework for easier digital certificate use", 2013. This system makes use of mobile optimized digital identity for digital certificate generation and authentication.

[3] Nwachukwu-Nwokeafor K.C, Igbajar Abraham, "Designing an Automatic Web Based Certificate Verification System for Institutions", 2015. The system can be used by an institution for its official website. The purpose of the system was to design online certificate system based on verification which can be used by the institution.

[4] Ravinder Reddy B, Pavan Kumar C, Rajrupa Singh, Selvakumar R, "Access Control and Data Security in Online Document Verification System", 2016. This online document verification system is based on Attribute Based Encryption (ABE). The system is aimed at providing access control for users to access the documents hosted on user's attributes.

[5] Sajan Ambadiyil, Haritha Sree G S, V.P.Mahadevan Pillai, "Facial Periocular Region based Unique ID Generation and One to One Verification for Security Documents", 2016. A unique ID is generated using facial periocular region, which is used for one to one verification of documents.

[6] Hamdi A. Ahmed, Jong-Wook Jang, "Higher Educational Certificate Authentication System Using QR Code Tag", 2017. The system makes use of QR code for authentication of digital certificates. The server database is used for the record of all generated QR codes.

[7] Ahmed Dalhatu Yusuf, Moussa Mahamat Boukar, Shahriar Shamilulu, "Automated Batch Certificate Generation and Verification System", 2017. Using client-server model, the system is developed which generates the certificates in batches and not individually.

III. SYSTEM ARCHITECTURE

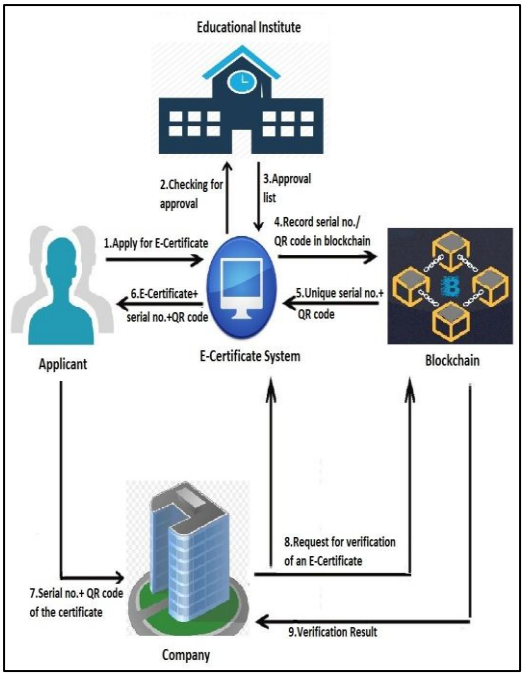

Figure 1. System Architecture

The working processes of the system is as follows:
1) Applicant requests for an E-certificate to the system.
2) Educational institute approves a degree certificate and enters the applicant's data into the system (i.e. blockchain). Then, the system stores the serial number of the applicant in a blockchain.
3) The certificate system verifies all the data.
4) Instead of sending hard copies, educational institute grant e-certificates containing a quick response (QR) code to the graduates whose data have been successfully verified.
5) When applying for a job, an applicant simply sends the serial number or e-certificate with a QR code to the company.
6) The company sends verification request to the system, which then gives verification result to the company.

IV. ADVANTAGES OVER OTHER SIMILAR SYSTEMS

The system assures valid E-certificate generation with accurate data of students. It saves the overhead of maintaining original documents. And importantly, provides an accurate verification of an E-certificate on the spot.

V. RESULTS AND DISCUSSION

Student needs to register first, then he can login and apply for a certificate by filling the required details (figures 2 and 3).

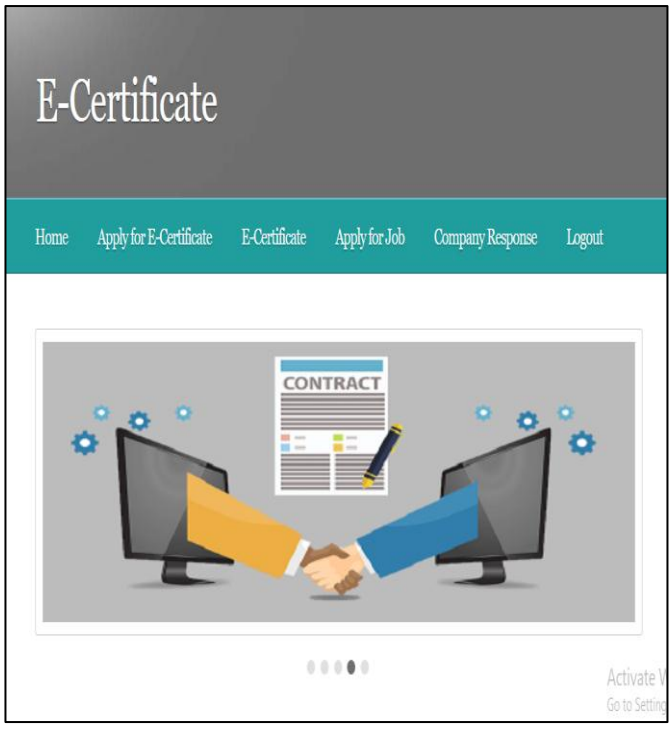

Figure 2. Student Homepage

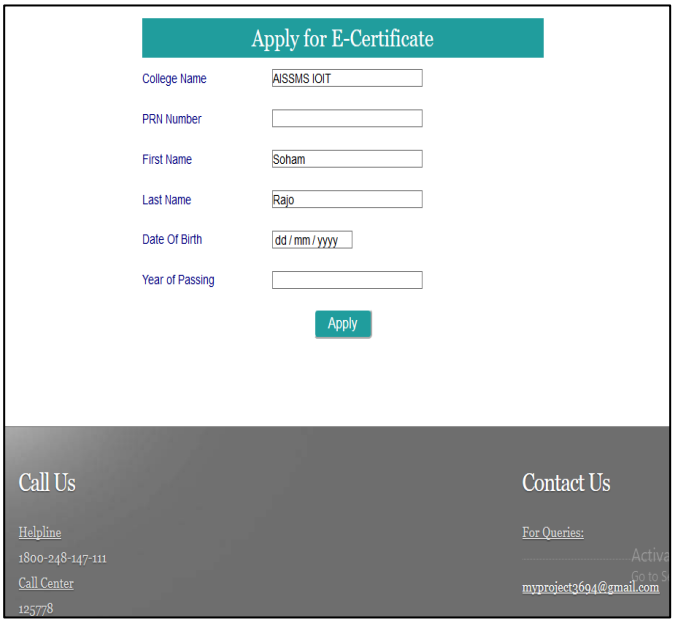

Figure 3. E-Certificate request from Student

Once a student requests for E-certificate, the request is validated by corresponding institute to make sure false certificates are not generated (figure 4).

Figure 4. Request Approval from College

The E-certificate generated will look like the one shown in figure 5.

Figure 5. E-Certificate

After receiving an E-certificate with QR code or serial number, one can apply for a job in desired company by providing the QR code to the company for verification (figure 6).

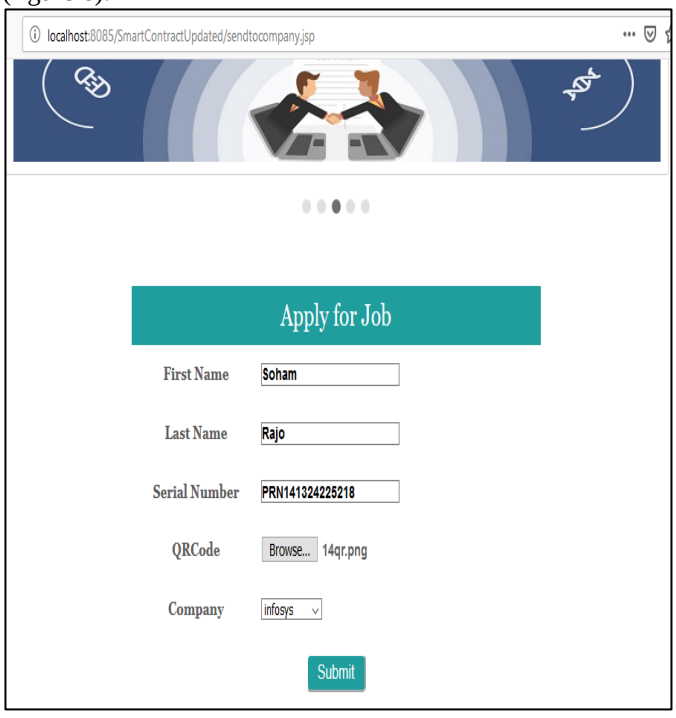

Figure 6. Job Application from Student

Then company at their side, can verify the authenticity of particular student by referring to the blockchain created (figure 7).

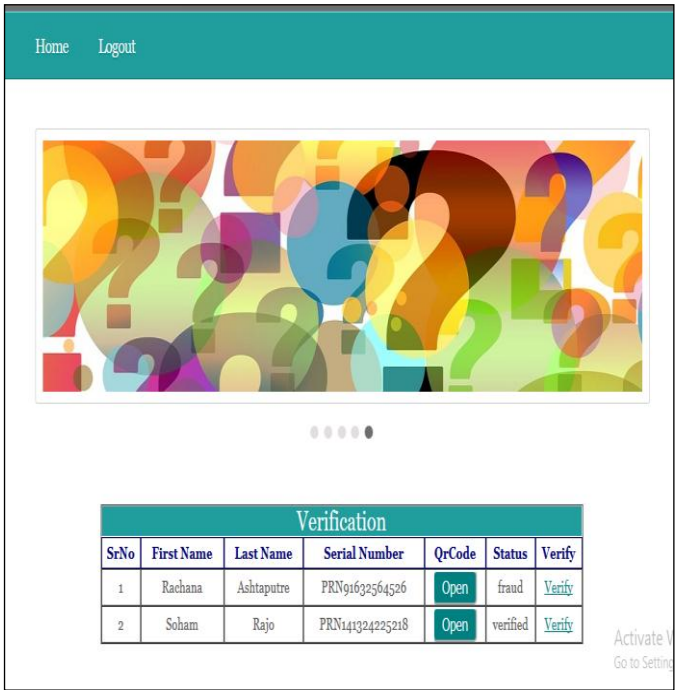

Figure 7. Job Application Verification (Company side)

VI. CONCLUSION AND FUTURE SCOPE

Our proposed system uses blockchain technology which is a distributed ledger means its each node stores and verifies the same data. Due to this feature of blockchain, our system enhances the credibility of the electronic files i.e. E-certificates and also reduces the chances of certificate forgery. The process of E-certificate application and its automated generation is very reliable and transparent. The demand units (i.e. company or organization) then, can inquire for the verification of information of the E-certificate with QR code or Unique serial number. The overall system assures information accuracy and security.

VII. ACKNOWLEDGMENT

We pay our thanks to Prof. Archana Said for providing a great support to us. She guided our project team efficiently. We successfully accomplished our work only due to her guidance.

REFERENCES

[1] Lein Harn and Jian Ren, "Generalized Digital Certificate for User Authentication and Key Establishment for Secure Communication", IEEE Transactions on Wireless Communications, Vol. 10, Issue 7, July 2011.
[2] C. V. Malone, E. J. Barkie, B. L. Fletcher, N. Wei, A. Keren, A. Wyskida, "Mobile Optimized Digital Identity (MODI): A framework for easier digital certificate use", IBM Journal of Research and Development, Vol. 57, Issue 6, December 2013.
[3] Nwachukwu-Nwoceafor K.C, Igbajar Abraham, "Designing an Automatic Web Based Certificate Verification System for

Institutions", Journal of Multidisciplinary Engineering Science and Technology (JMEST), Vol. 2, Issue 12, December 2015.

[4] Ravinder Reddy B, Pavan Kumar, "Access Control and Data Security in Online Document Verification System", In the proceedings of 2016 IEEE International Conference on Computational Intelligence and Computing Research (ICCIC), India, 2016.

[5] Sajan Ambadiyil, Haritha Sree G S, V.P.Mahadevan Pillai ,"Facial Periocular Region based Unique ID Generation and One to One Verification for Security Documents", In the proceedings of 2016 2nd International Conference on Advances in Electrical, Electronics, Information, Communication and Bio-Informatics (AEEICB), India, 2016.

[6] Hamdi A. Ahmed, Jong Wook Jang, "Higher Educational Certificate Authentication System Using QR Code Tag", International Journal of Applied Engineering Research, Vol. 12, Issue 20, 2017.

[7] Ahmed Dalhatu Yusuf, Moussa Mahamat Boukar, Shahriar Shamiluulu, "Automated Batch Certificate Generation and Verification System", In the proceedings of 2017 13th International Conference on Electronics, Computer and Computation (ICECCO), Nigeria, 2017.

[8] N.S.Tinu, "A Survey on Blockchain Technology- Taxonomy, Consensus Algorithms and Applications", International Journal of Computer Sciences and Engineering(IJCSE), Vol. 6, Issue 5, May 2018.

[9] Jiin-Chiou Cheng, Narn-Yih Lee, Chein Chi, Yi-Hua Chen, "Blockchain and Smart Contract for Digital Certificate", In the proceedings of IEEE International Conference on Applied System Innovation 2018(ICASI), Japan, 2018.

[10] Guang Chen, Bing Xu, Manli Lu and Nian-shing Chen, "Exploring blockchain technology and its potential application for education", Springer Open- Smart Learning Environments Journal, 2018.

AUTHOR'S PROFILE

Ms. Payal Dhamale is currently pursuing Bachelor of Computer Engineering from AISSMS's Institute of Information Technology, affiliated to Savitribai Phule Pune University in year 2019. The paper is in her interest of research work in the domain of data security.

Ms. Rachana Ashtaputre is currently pursuing Bachelor of Computer Engineering from AISSMS's Institute of Information Technology, affiliated to Savitribai Phule Pune University in year 2019. She has done her research work in data security field as a part of the case study based on the same concept which is represented in the paper.

Ms. Srushti Bandal is currently pursuing Bachelor of Computer Engineering from AISSMS's Institute of Information Technology, affiliated to Savitribai Phule Pune University in year 2019. As a part of the course curriculum, she chose to work on data security and studied the topic. Based on that, put her research work in the paper.

Ms. Babita Bisht is currently pursuing Bachelor of Computer Engineering from AISSMS's Institute of Information Technology, affiliated to Savitribai Phule Pune University in year 2019. Her interest in the domain of data security made her do some research work and put it in here.

