CERTIFICATE VALIDATION USING BLOCKCHAIN

M. Sravan Kumar Babu[1], B. Vaishnavi[2], K. Akshitha[2], M. Sruthi[2], Ch. Nikitha[2]

[1]Assistant Professor, [2]UG Scholar, [1,2]Department of CSE-Cyber Security

[1,2]Malla Reddy Engineering College for Women (A), Maisammaguda, Medchal, Telangana.

ABSTRACT

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: Certificate validation, Blockchain, Security.

1. INTRODUCTION

Block chain was introduced in the year 2008 by Satoshi Nakamoto. Block chain 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. Block chain is the main tool to felicitate this need and when combined with different hashing techniques, this becomes a powerful method for protecting the data. It also helps in eliminating the need for constant verification of certificates. Block chain technology is used to reduce the incidence of certificate forgeries and ensure that the security, validity, and confidentiality of graduation certificates would be improved. Technologies that exist in security domains include digital signatures, which are used in digital documents to provide authentication, integrity, and non- repudiation. Also with block chain in play, the storage of certificates are more secure. With these technologies, an application created that facilitates the secure validation of digital certificates.

2. LITERATURE REVIEW

Blockchain and Smart Contract for Digital Certificate

Author: Jiin-Chiou Cheng; Narn-Yih Lee; Chien Chi; Yi-Hua Chen

Due to the lack of effective anti-forge mechanism, events that cause the graduation certificate to be forged often get noticed. In order to solve the problem of counterfeiting certificates, the digital certificate system based on blockchain technology would be proposed. By the unmodifiable property of blockchain, the digital certificate with anti-counterfeit and verifiability could be made.

Blockchain-Based Certificate Transparency and Revocation Transparency Author: Ze Wang; Jingqiang Lin; Quanwei Cai; Qiongxiao Wang

In this article, we propose blockchain-based certificate transparency (CT) and revocation transparency (RT) to balance the absolute authority of CAs. Our scheme is compatible with X.509 PKIs but significantly reinforces the security guarantees of a certificate. The CA-signed certificates and their revocation status information of an SSL/TLS web server are published by the subject (i.e., the web server) as a transaction in the global certificate blockchain. The certificate blockchain acts as append-only public logs to monitor CAs' certificate signing and revocation operations, and an SSL/TLS web server is granted with the cooperative control on its certificates.

Blockchain and Smart Contract for Digital Document Verification

Author: S. Sunitha kumari Saveetha Dhandapani

Due to lack of anti-forge mechanism some started to forge the certificate to get the employed or for further steps. In the digital certificate verification based on blockchain done only for the degree certificates. In the proposing system along with the degree certificate entire personality and behaviour activities of the person using personal id will be uploaded in blockchain.

Issuing and Verifying Digital Certificates with Blockchain

Author: Trung Tru Huynh, Dang Khoa Pham, Anh Khoa Ngo

In this study, we propose and implement an issuing and verifying model called UniCert based on Uni Coin which is a digital currency built on the blockchain technology. Our diagram can be extended to address many other issues such as anti- counterfeiting, copyright protection of music products, patents, etc.

Tamper Proof Birth Certificate Using Blockchain Technology

Author: Maharshi Shah, Priyanka Kumar

Nowadays birth certificate is the only age proof of an individual and can be used to apply for a job, for admissions in collages/universities and basis of all the important government document identities like Aadhar card, Pan Card, Passport and other related matters. So identifying the correct birth certificate of any person is a major challenge. In the current system, afterbirth of any individual the birth has to be registered with the concerned local authorities within 21 days of its occurrence, then it should be filled up the form prescribed by the Registrar and then Birth Certificate is issued after verification with the actual records of the concerned hospital. However, current methodology used for birth certificate verification is costly and very time consuming.

3. PROPOSED SYSTEM

A. Methodology

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.

B. Digital Certificate Creation

In this, the student certificates are converted into digital certificates. The academic certificate and sports certificate are issued by the institution are stored in the database. By using the analog image to digital image conversation method the certificate can be converted into a digital certificate.

C. Hash Code Generation

When the certificate is uploaded, the hash value is created for the digital certificate. Compared to SHA-1, the chaotic hash function are collision resistant.

D. Digital certificate validation

In this, the created digital certificate is validated. Certificates that are stored in the blockchain are validated by matching the hash value. The verification of the hash value of the certificate is used to avoid tampering.

E. Working of Application

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.
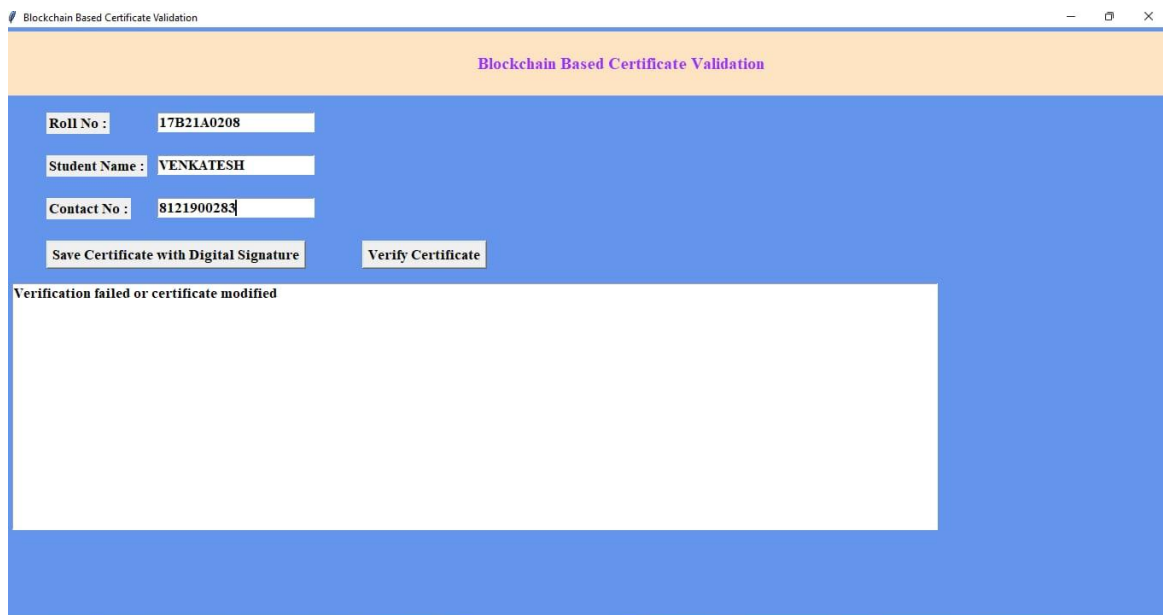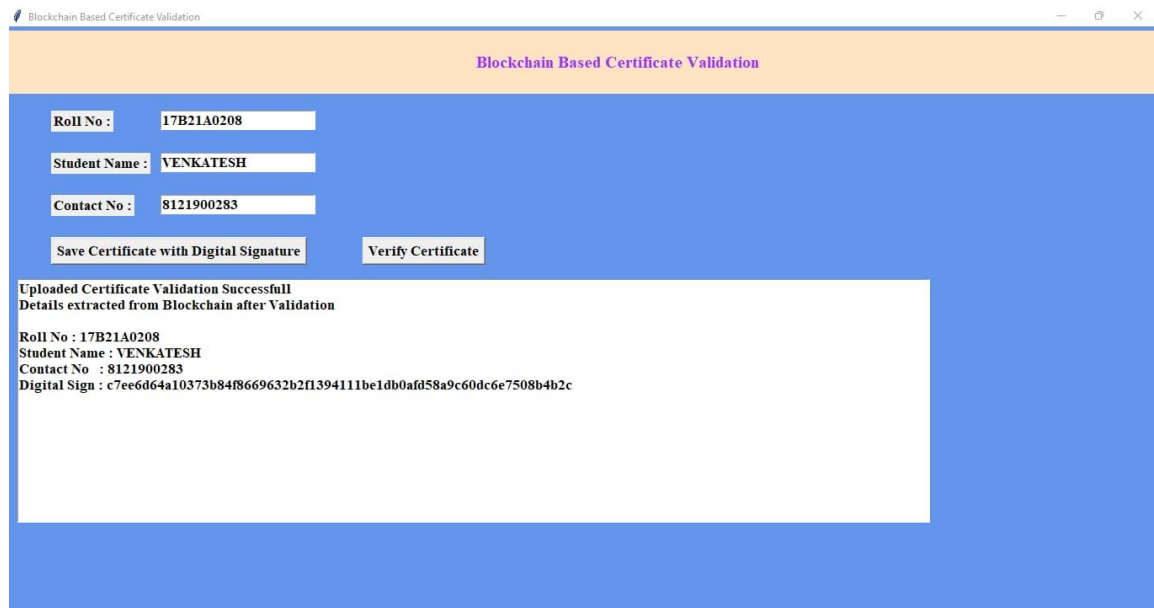
Advantages

By using the analog image to digital image conversation method the certificate can be converted into a digital certificate.

4. RESULTS
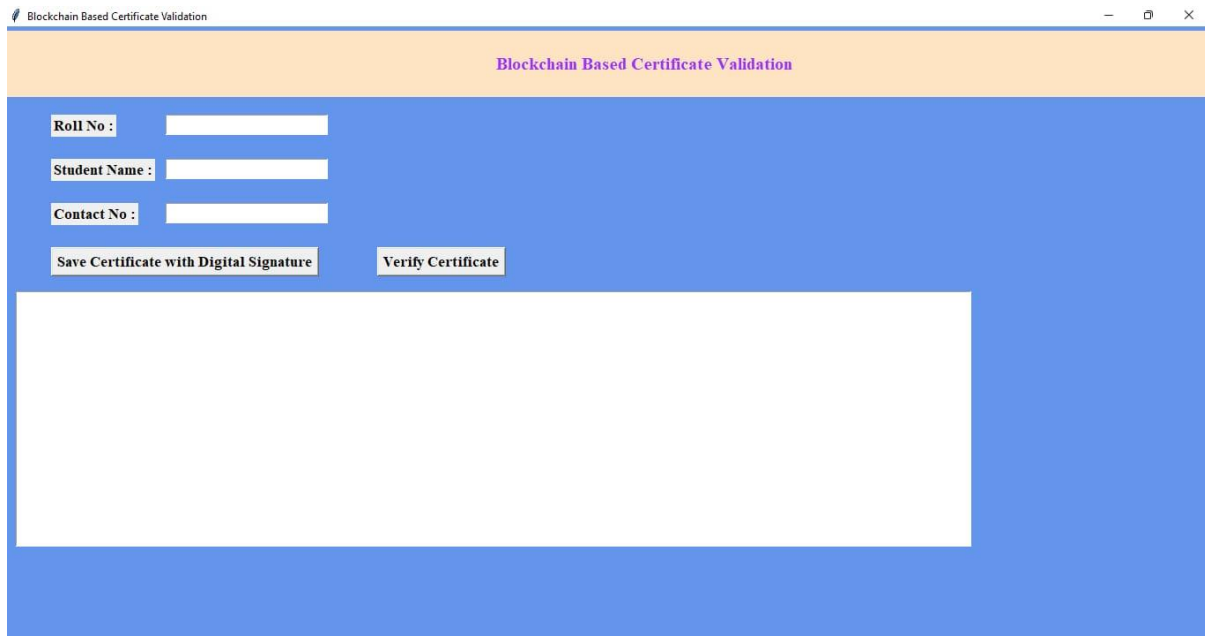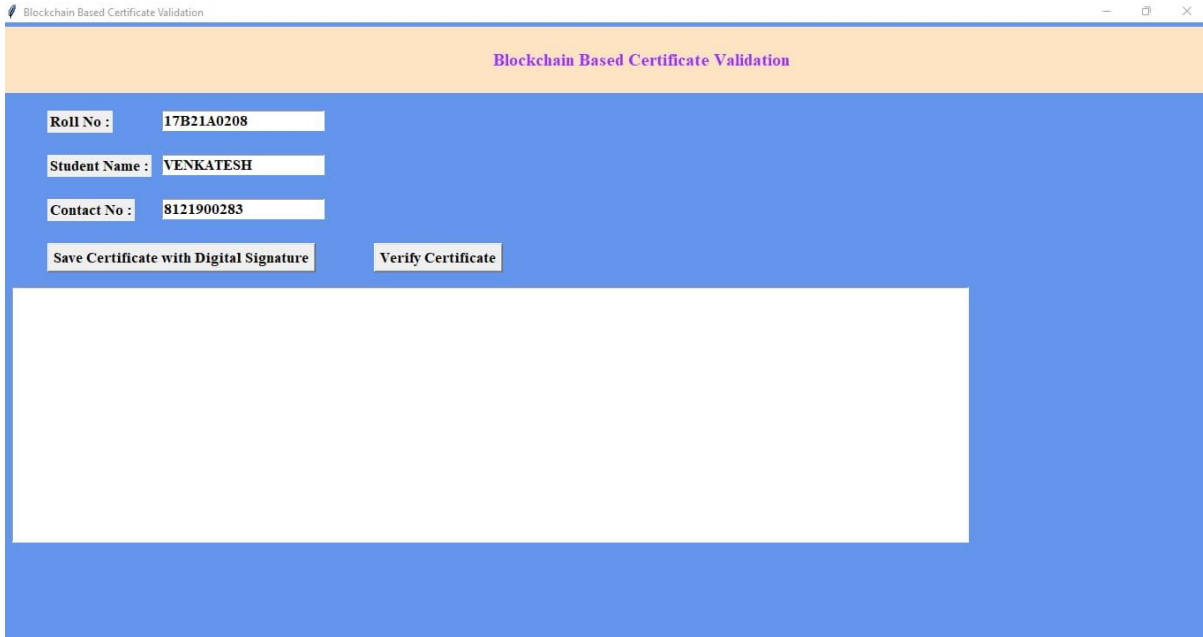
5. CONCLUSION

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.

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", Journal of Physics: Conference Series, Volume 1069, 3rd Annual International Conference on Information System and Artificial Intelligence (ISAI2018) 22–24 June 2018, Suzhou.

[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 20 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.

[9] Trong Thua Huynh, Trung Tru Huynh, Dang Khoa Pham, Anh Khoa Ngo, "Issuing and Verifying Digital Certificates with Blockchain" https://dx.doi.org/10.1109/ATC.2018.8587428.

[10] Maharshi Shah, Priyanka Kumar, "Tamper Proof Birth Certificate Using Blockchain Technology" International Journal of Recent Technology and Engineering (IJRTE).