How to Cite:
Ahmmed, M. M., Nooruddin, M. S., Asimuddin, M., & Samad, S. A. (2022). Certificates verification on the block chain. *International Journal of Health Sciences*, *6*(S8), 835–843. https://doi.org/10.53730/ijhs.v6nS8.9809

Certificates verification on the block chain

Mr. Mohammed Mateen Ahmmed
Assistant Professor, Department of Information Technology, Lords Institute of Engineering &Technology, Jawaharlal Nehru Technological University, Hyderabad (JNTUH)

Mohammed Shaik Nooruddin
B.Tech. Student, Department of Information Technology, Lords Institute of Engineering &Technology, Jawaharlal Nehru Technological University, Hyderabad (JNTUH)

Mohd Asimuddin
B.Tech. Student, Department of Information Technology, Lords Institute of Engineering &Technology, Jawaharlal Nehru Technological University, Hyderabad (JNTUH)

Syed Abdul Samad
B.Tech. Student, Department of Information Technology, Lords Institute of Engineering &Technology, Jawaharlal Nehru Technological University, Hyderabad (JNTUH)

***Abstract*---**All certificates, including those for secondary school graduation, high school diplomas, and college degrees, have been converted to digital form and made accessible to students at higher education institutions. It's essential for learners to keep track of their diplomas. It is a complex and time-consuming process for the institution or organization to verify or authenticate a certificate's validity. This application would aid in the safekeeping of the certificates on the block chain. Digital certificates are created by first digitising the original paper certificates. The certificate's hash code value is generated using the chaotic technique. It is then added to the block chain. The mobile application is used to verify these certifications. We can make digital certificate verification more reliable and safe by implementing block chains.

***Keywords*---**complex technique, hashing, digital certificates, block chain.

Introduction

Satoshi Nakamoto, a mysterious figure who first appeared on the block chain in 2008, announced the technology's existence. Distributed as well as accessible information exchange can be achieved through the use of Block chain, one of the internet accounting records [3]. We are creating an Android app to securely verify our certifications as phase of this project. Persons could now readily alter details on graduating credentials including records in ways that must be impossible for outsiders to access. The need for an effective mechanism to ensure that the information in such certifications is genuine[1], essentially indicates that the documents originates out of a trusted and approved sources[6] and is not faked, is considerable. E-certificates for educational establishments can be safely stored in the cloud using a variety of techniques [2]. With diverse hashing technologies mixed with block chain, this offers an extremely strong means for securing data. It also reduces the requirement for certifications to be verified on a regular basis [9]. Certificate forgery can be reduced and the privacy, authenticity, and secrecy of graduation certifications can be improved using block chain technology. Digital certificates, which are employed in digital information for authenticating, consistency, and non-repudiation, are among the encryption technology that exists [8]. The storing of certifications has always been more secured with using block chain [10]. Digital certificates can be validated safely using a technology is a growing through these techniques.

Related work

To create a digital certification using block chain - based smart contracts

There are around one billion students in Taiwan every year according to the Ministry of Education estimates, most of whom will advance their careers at higher education institutions & college administrators, while others will be prepared to begin the workforce. In the course of the program, graduates' certifications, papers, and degrees would serve as crucial references when applying to new institutions or bringing in new responsibilities [4]. All that's needed to create certificates and diplomas is the student' and institutions' identities. Fabricated graduating certificates are kinds of items because of the absence of an effective anti-forge device [6]. The blockchain-based digital certificate scheme would've been presented to address the issue of certificate forgery. Because of blockchain's immutable nature, it is possible to create a digital certificate that is both pro government and verifiable [5]. This platform's digital identity issuance process looks like this: After generating a digital file of a papers certification and calculating the digital application's hash code, upload the digital file to the databases. To wrap things up, add the hash function to a new block in the chain. QR codes and inquiring strings codes would be printed on the paper certificate by the software. The demanding unit could use Smartphone scanners or internet enquiries to validate the papers certificate's legitimacy. In addition to enhancing the legitimacy of different journal article certifications, the platform simultaneously digitally reduced the chance of losing different kinds of certifications.

Block chain-Based Decentralised Digital Certification Provision

If you have several certification authorities (CAs), today's digital certifications revoking mechanisms are inadequate, combined with a lack of interpersonal trust, access security as well as the timely synchronisation of information. In this paper, we present a blockchain-based digitally signed non - repudiation system that relies on a total secrecy block chain network. To ensure the safety of the user information & properties, it has the ability to revoke the digital certificate. [7] The system's core technology is consortia decentralized crypto currency, which is based on the block chain consensus mechanism's properties. It is possible to create the educational assistance condition protocol (OCSP) on the basis of this technology, which enables various certificates (CAs) to work together to manage certificate authority revoke lists (CRLs). This method is impenetrable, safe, and efficient. CRL over several CAs is more trustworthy and reliable than previous methods of certificates revoking, allowing for a wider range of applications of block chain.

From Presentations of the First Italian Convention on Cyber security, Certification Verification via Public Ledger accounts and Block chains

Authentication applications such as e-commerce, e-government, internet banking, mail, networking websites, other cloud storage all reliant on external key architectures (PKIs). PKIs are critical to the survival among several internet services. Cert revocation lists (CRLs), which are required to be maintained and authenticated each moment a certificates is used, are one of the primary threats to the system (POFs) of current PKIs. There is a single point of failure (POF) in a system where its CRL for just a collection of certifications is managed by another (and sole) certificate holder (CA). Several CAs can pool their CRLs into one accessible, decentralised, more secure block chain to solve this problem. For this, we'll look at the block chain-based public ledger concept, which was originally developed for usage in crypto currencies but is now being adopted by a wide range of web applications requiring high demands on accuracy and protection.

Using Block chain to issue and verify digital certificates

To build and operate shared systems and save transaction details without any need for third party to verify it, block chain technology has already been used in many ways. Management of educational institutions all around the world are particularly interested in the subject of fake certification. It has been a major issue thus far. Because of this, implementing a block chain-based system to issue and validate digital certificates [4] will fix the problems of fraudulent certifications, which has never been addressed by any preceding technology. An issuing and verifying methodology called Unicorn is proposed and implemented in this study using Unicorn, a crypto currency founded on the block chain technology. Many other problems, such as anti-counterfeiting, copyrighted material for music items, trademarks, and so on, can be addressed using our model.

Methodology

As part of this plan, we are transforming all educational certificate of registration into digital certificates, which become saved in a Block chain device that supports adulterate storage devices, ensuring that no one has access to and can actually change its information. If, for some reason, the information in the Block chain device is altered, the verification system would then struggle and users would be notified.

If this site alters transactions, some other servers would be able to tell since the hash code for the identical information would be changed on each of the remaining servers [7]. It is possible to stop future suspicious changes to the information by storing it on data centres, such as in Distributed ledger technology, where information is recorded on various computers and if an unauthorized attacker alters information solely on a single domain controller, that server's type of encryption would be transformed and another data centres would then remain unchanged. If existing hash codes behave identically, the information is considered genuine & unmodified, and fresh data information is added to the Blockchain as a new part on the Internet. Every block hash code would be validated after every new data repository.

Digital Certificate Creation: Here, student certifications are turned into electronic signatures. The organisation's dataset includes the educational certification and sporting certification granted mostly by institute. The certification could be turned into a certificate authority utilising the analogue picture to digital photo way of communication. Every certification has its own set of 0s and 1s. All 2-dimensional functional parameters with their accompanying variables were limited in a digital photo. A pixels can defined as a single integer. By logging in as an administration, the executive can upload a person's certification to our program, which then uses samples and quantized to transform the analogue image into a digital one. Students can be added and certificates can be added on the following page. Students are registered if an administrator tapes in the new student. The student's certification is downloaded if an administrator hits the "Add Certificates" button.

Hash Code Generation: The certificate's hash value is generated using a chaotic method. Using this approach, you can input data in a variety of formats and get the same result. The translation strategy, initial values, and variables of this method must be specified. A same set of initial conditions and settings is used to obtain the same output during the verification procedure. The hash function for the certificate authority is generated whenever the certification is submitted. The chaotic hash algorithm is more collision resistant than SHA-1.

Digital certificate validation: In this case, the digital identity that was generated is verified. In the block chain, certifications can be verified by comparing their hash values. To prevent tampering, the certificate's hash function is checked. You may sign in with the programme by entering your login details. They can choose the sort of certificate they want to verify. The verify checkbox should be taped to the program. To ensure that the certificate is authentic, the outcome should be a

validated certification. The result would be errors as well as revised certification if indeed the certification isn't genuine or has been altered in any way.

Working of Application: There is an administrator login page, a page for adding students and certificates, and a page for verifying credentials. Our programme allows the administrator to log in using the administrator login id and password. The administrator could then use the add students as well as certification buttons to enter the student's information. Next, the validated could use verification access username and passwords to verify the certification. They enter the participant's e-mail address and click the "verify" tab. The outcome would be successful if the certifications that were submitted are authentic. Errors & modifications would be the final outcome if this is not done.

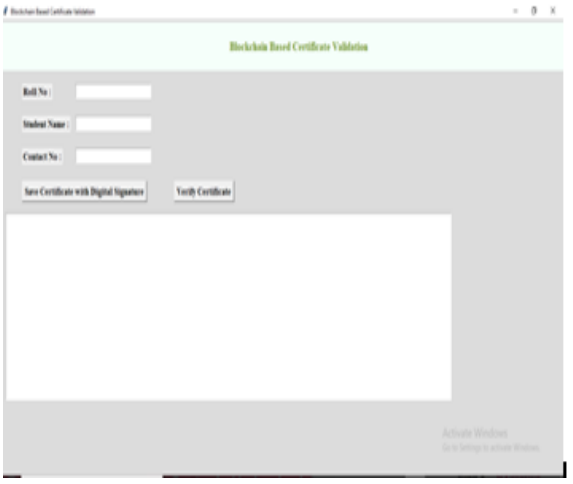
The following modules have been developed as phase of this project:

Save Certificate with Digital Signature: When a student's educational credential is uploaded, the programme converts the certification into a digital certificate, which is recorded in the Block chain database together with the student's personal information.

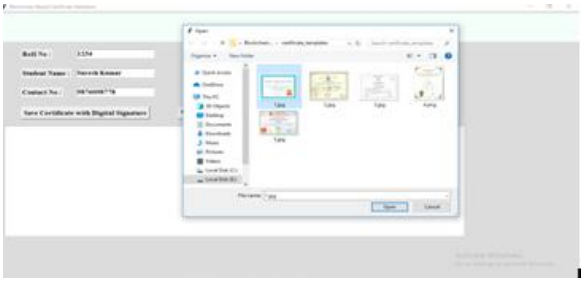
Verify Certificate: If a match is found, the Block chain dataset would then collect all student information and demonstrate them to the valuator; if a correlation is not discovered, the credential is considered insincere or start building. This feature includes a verification system, a company, or an administrator to collect the certificate from a student and submit it to the implementation, which then converts it into a digital signature.

Result and Discussion

In order to run code, simply double-click on the run file.

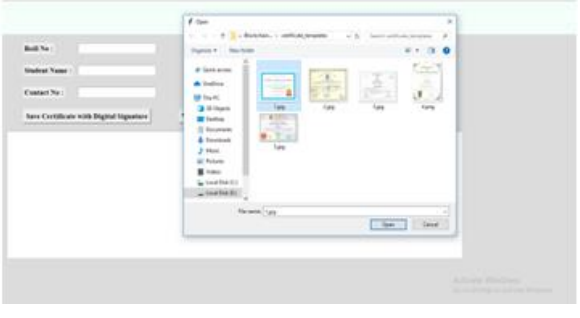


Insert the student's information in the field provided ahead, and afterwards clicking labelled "Store Certificates using Digital Certificates" that will save the certification as a digital certificate.



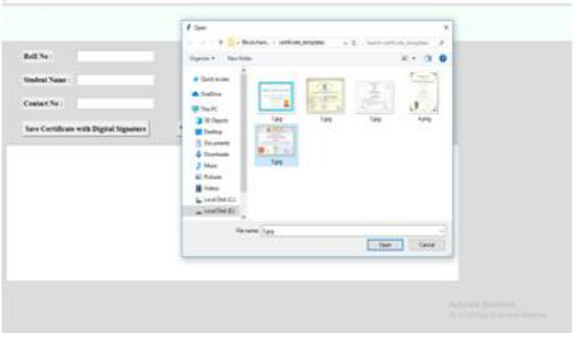
After completing the above steps, press on the 'Save Certificate using Digital Signature' tab and afterwards pick and uploading '1.jpg' file, and thereafter clicking on the "Open" tab.

Although Blockchain creates additional block with every certification uploading, you could see that the old and new hashing codes are checked against another to ensure that all information has not been altered. As a result, the information listed above is now saved in the block chain, and anyone may validate it by clicking the "Verify Certificate" tab and uploading the picture listed follows.



When you clicking on the "Open" tab in the outcomes displayed above, you'll see the information seen below.

App verified digital signature from Block chain technology now and trying with other input image to see if it is possible to identify it.



This result is obtained by first loading the "5.jpg" file to your computer and afterwards clicking the tab labelled "Open."

Validation was unsuccessful because the submitted certificate didn't reflect the saved certifications in the Block chain, as shown in the above reports. It's possible to create a digital certificate from virtually anything certification you supply.

Conclusion

In this work, we present a block chain-based solution to these problems of certificate forging. It's critical that the information you're working with is safe. We may improve information privacy as well as prevent certification forgeries through exploiting the unchallengeable quality of block chain. The user can access and

verify the certification through the program. This method ensures the quality and security of the information while also making it simple for users to administer digital certificates.

References

1. Jiin-Chiou Cheng; Narn-Yih Lee; Chien Chi; Yi-Hua Chen, "Block chain 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) Block chain-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 Block chain," 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 Block chain", 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. Thammana Ajay, K Nagi Reddy, Dasari Anantha Reddy, Pattem Sampath Kumar, K Saikumar, "Analysis on SAR Signal Processing for High-Performance Flexible System Design using Signal Processing" in proceedings of 5th International Conference on Electronics, Communication and Aerospace Technology (ICECA) held during 02-04 December 2021, pp.30-34.
8. V Jothsna, Ibrahim Patel, K Raghu, P Jahnavi, K Nagi Reddy, K Saikumar, "A Fuzzy Expert System for The Drowsiness Detection from Blink Characteristics", in proceedings of 7th International Conference on Advanced Computing and Communication Systems (ICACCS) held during 19-20 March 2021, pp.1976-1981.
9. Kumar, S. (2022). A quest for sustainium (sustainability Premium): review of sustainable bonds. Academy of Accounting and Financial Studies Journal, Vol. 26, no.2, pp. 1-18
10. Allugunti V.R (2022). A machine learning model for skin disease classification using convolution neural network. International Journal of Computing, Programming and Database Management 3(1), 141-147
11. Allugunti V.R (2022). Breast cancer detection based on thermographic images using machine learning and deep learning algorithms. International Journal of Engineering in Computer Science 4(1), 49-56
12. 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.

13. Maharshi Shah, Priyanka Kumar, “Tamper Proof Birth Certificate Using Blockchain Technology” International Journal of Recent Technology and Engineering (IJRTE).
14. Widana, I.K., Sumetri, N.W., Sutapa, I.K., Suryasa, W. (2021). Anthropometric measures for better cardiovascular and musculoskeletal health. *Computer Applications in Engineering Education*, *29*(3), 550–561. https://doi.org/10.1002/cae.22202
15. Novoa, R. B. (2021). State of the art and future applications of digital health in Chile. *International Journal of Health & Medical Sciences*, *4*(3), 355-361. https://doi.org/10.31295/ijhms.v4n3.1772