BLOCK CHAIN BASED CERTIFICATE VALIDATION

D.M.Rafi
Assistant Professor
Department Of CSE
CVRT Engineering college, Tadipatri.

C.Siva
Assistant Professor
Department Of CSE
CVRT Engineering college, Tadipatri.

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.

I. INTRODUCTION

Advances in information technology, the wide availability of the Internet, and common usage of mobile devices have changed the lifestyle of human beings. Virtual currency, digital coins originally designed for use online, has begun to be extensively adopted in real life. Because of the convenience of the Internet, various virtual currencies are thriving, including the most popular—Bit coin, Ether, and Ripple —the value of which has surged recently. People are beginning to pay attention to block chain, the backbone technology of these revolutionary currencies. Block chain features a decentralized and incorruptible database that has high potential for a diverse range of uses. Block chain is a distributed database that is widely used for recording distinct transactions. Once a consensus is reached among different nodes, the transaction is added to a block that already holds records of several transactions. Each block contains the hash value of its last counterpart for connection. All the blocks are connected and together they form a blockchain. Data are distributed among various nodes (the distributed data storage) and are thus decentralized. Consequently, the nodes maintain the database together. Under blockchain, a block becomes validated only once it has been verified by multiple parties. Furthermore, the data in blocks cannot be modified arbitrarily. A blockchain-based smart contract, for example, creates a reliable system because it dispels doubts about information's veracity. Because information technology has developed rapidly in recent years, data protection is more necessary than ever.

Graduates, whether they choose to continue studying or start job hunting, require various certificates for interviews. However, they often find that they have lost their educational and commendation certificates. Reapplying for hard copies can be time-consuming because certificates are granted by different organizations and in-person application may be necessary. By contrast, applying for an e-copy can save paper and time. By providing information for identity verification, graduates are able to apply for any certificate easily. Nevertheless, because of this convenience,

forged degree certificates, licenses, and certificates are prevalent. Consequently, schools and companies cannot instantly validate the documents they receive. To solve this problem, a certificate system based on block chain was designed in this study. Data are stored in different nodes, and anyone who wishes to modify a particular internal datum must request that other nodes modify it simultaneously. Thus, the system is highly reliable.

In this study, we developed a decentralized application and designed a certificate system based on E/there umblockchain. This technology was selected because it is incorruptible, encrypted, and trackable and permits data synchronization. By integrating the features of blockchain, the system improves the efficiency operations at each stage. The system saves on paper, cuts management costs, prevents document forgery, and provides accurate and reliable information on digital certificates.

1.1 Objective of the project:

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.

II. LITERATURE SURVEY:

Verification and Validation of Certificate Using Blockchain

According to the Indian Ministry of Education statistics, document verification is a complex domain that involves various challenging and tedious processes to authenticate. Due to the lack of an 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. For students, educational certificates are the most important documents issued by their universities. However, as the issuing process is not that transparent and verifiable, fake certificates can be easily created. A skillful generated fake certificate is always hard to detect and can be treated as the original. With the increase of forged documents, the credibility of both the document holder and the issuing authority is jeopardized. In order to solve the problem of counterfeiting certificates,the digital certificate system based on blockchain technology would be proposed. By the modifiable property of blockchain, the digital certificate with anti-counterfeit and verifiability could be made. The procedure of issuing the digital certificate a in this system is as follows. First, generate the electronic file of a paper certificate accompanying other related data into the database, meanwhile; calculate the electronic file for its hash value. Finally, store the hash value into the block in the chain system. In this research, the authors have identified the security themes required for document verification in the blockchain.This research also identifies the gaps and loopholes in the current blockchain-based educational certificate verification. The system

will create a related QR-code and inquiry string code to affix to the paper certificate. It will provide the demand unit to verify the authenticity of the paper certificate through mobile phone scanning or website inquirie

Design And Develop Certificate Validation System Using Smart Contract

Blockchain is an emerging technology that has the potential to revolutionize the global industry and create a trusted relationship in a multi-party business network. Block-chain is one of the most stable open ledgers that preserves transaction information, and is difficult to forge. Since the information stored in block-chain is not related to personally identifiable information, it has the characteristics of anonymity. There are a number of practical use cases where blockchain has been applied. Throughout the educational course students receives various kind of performance certificates, score transcript, mark sheets etc which can become an extremely important attribute for having admissions to new schools or new works. Due to anti-forge mechanism, its easy to make fake documents. To solve the problem of fraudulent certificates, the digital certificate system based on block chain technology would be proposed. By the un modifiable property of block chain , the digital certificate with anti-counterfeit and verification could be made. Through the un modifiable properties of the block chain, the system not only enhances the credibility of various paper based certificates, but also electronically reduces the loss risks of various types of certificates.

Generating E-Certificate and Validation using Blockchain

Lakhs of people getting Degrees year after year, due to the lack of effective anti-forge mechanism, events that cause the graduation certificate to be forged often get noticed. according to the Indian Ministry of Education statistics, document certify of of document verification is a complex domain that involves various challenging and tedious processes to authenticate. Certificate of Blockchain is a large and open-access online ledger in which each node saves and verifies the same data. Using the proposed system manual proposed block chain based system reduces the Like hood of certificate forgery. The processes of generation certificate granting are open and transparent in the system. Due to the lack of an 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 block chain technology would be proposed. For students, educational certificates are the most important documents issued by their universities. However, as the issuing process is not that transparent and verifiable, fake certificates can be easily created. A skillful generated fake certificate is always hard to detect and can be treated as the original. With the increase of forged documents, the credibility of both the document holder and the issuing authority is jeopardized. In order to solve the problem of counterfeiting certificates,the digital certificate system based on blockchain technology would be proposed. By the modifiable property of blockchain, the digital certificate with anti-counterfeit and verifiability could be made. The procedure of issuing the digital certificate a in this system is as follows. First, generate the electronic file of a paper certificate accompanying other related data into the database, meanwhile; calculate the electronic file for its hash value. Finally, store the hash value into the block in the chain system. In this research, the authors have identified the security

themes required for document verification in the blockchain.This research also identifies the gaps and loopholes in the current blockchain-based educational certificate verification. The system will create a related QR-code and inquiry string code to affix to the paper certificate. It will provide the demand unit to verify the authenticity of the paper certificate through mobile phone scanning or website inquiries.

Integration of Digital Certificate Blockchain and Overall Behavioural Analysis using QR and Smart Contract

The Main purpose of this study is to develop a theoretical framework for blockchain. Our aim is to identify the barriers and main drivers of digital innovation and explore the possibilities of applications of blockchain. A case study approach is applied: the Norwegian offshore industry. Primary data is collected through the interviews and secondary data is collected from reports of industries and companies, the Internet, and national and international media reports. We have discovered that intensions of cost reduction, and the amount of large data that maritime companies should process, along with the effective work intension, are the main drivers of digital innovation. On the other hand, the bad quality of internet, high cost implementation, the technology-oriented culture, the lack of investment initiatives, and risk aversion are the main barriers. Some of the barriers and motives of digital innovation and the introduction to blockchain technology were pointed out by earlier studies. However, we have identified many unique drivers and barriers specific to the industry. Finally, the framework of blockchain process developed.

Blockchain and Smart Contract for Digital Document Verification

Every year lakhs of students graduating from different university, after passing from university different students have different plans. All students who graduated will have different certificate such as marksheets, degree certificate, best performance certificate and etc. Some students have plans to get employed in companies or to do higher studies. Wherever students go they need submit the certificate for important reference. 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. Because of unmodifiable property it is stored in block chain. Initially the student request for the e-certificate by uploading certificate or personal id to electronic certificate system. If requesting for e-cert then the system will review certificate from the university or schools or from organization and get the assurance and store the serial number and e-certificate to the block chain. The system will be generating the QR code and send it to the user. when applying for company user will send only the certificate serial number and QR code received from the e-certificate company

Blockchain for Electronic Voting System—Review and Open Research Challenges

Online voting is a trend that is gaining momentum in modern society. It has great potential to decrease organizational costs and increase voter turnout. It eliminates the need to print ballot papers or open polling stations—voters can vote from wherever there is an Internet connection. Despite these benefits, online voting solutions are viewed with a great

deal of caution because they introduce new threats. A single vulnerability can lead to large-scale manipulations of votes. Electronic voting systems must be legitimate, accurate, safe, and convenient when used for elections. Nonetheless, adoption may be limited by potential problems associated with electronic voting systems. Blockchain technology came into the ground to overcome these issues and offers decentralized nodes for electronic voting and is used to produce electronic voting systems mainly because of their end-to-end verification advantages. This technology is a beautiful replacement for traditional electronic voting solutions with distributed, non-repudiation, and security protection characteristics. The following article gives an overview of electronic voting systems based on blockchain technology. The main goal of this analysis was to examine the current status of blockchain-based voting research and online voting systems and any related difficulties to predict future developments. This study provides a conceptual description of the intended blockchain-based electronic voting application and an introduction to the fundamental structure and characteristics of the blockchain in connection to electronic voting. As a consequence of this study, it was discovered that blockchain systems may help solve some of the issues that now plague election systems. On the other hand, the most often mentioned issues in blockchain applications are privacy protection and transaction speed. For a sustainable blockchain-based electronic voting system, the security of remote participation must be viable, and for scalability, transaction speed must be addressed. Due to these concerns, it was determined that the existing frameworks need to be improved to be utilized in voting systems.

Securing e-voting based on blockchain in P2P network

Electronic voting (e-voting) is an electronic means for casting and counting votes. It is an efficient and cost-effective way for conducting a voting procedure, which has characteristic of being magnanimous data and real time and requesting high safety. However, concerns on security of networking and privacy of communication for e-voting have been grown. Securing e-voting is very urgent and has becoming a popular topic in the area of communications and networking. We present techniques to exploit blockchain in P2P network to improve the security of e-voting. First, we design a synchronized model of voting records based on distributed ledger technology (DLT) to avoid forgery of votes. Second, we design a user credential model based on elliptic curve cryptography (ECC) to provide authentication and non-repudiation. Third, we design a withdrawal model that allows voters to change their vote before a preset deadline. By integrating the above designs, a blockchain-based e-voting scheme in P2P network is proposed for essential requirements of e-voting process. To prove and verify the scheme, a blockchain-based e-voting system for multiple candidates has been designed on Linux platforms in P2P network. The system involves electronic voting theory, cryptography, and software engineering theory. The implementation result shows that it is a practical and secure e-voting system, which solves the problem on forgery of votes during e-voting. The blockchain-based e-voting system can be applied to a variety of networking applications directly.

An Empirical Study of Online Shopping Using Blockchain Technology

This study specifically explores whether user acceptance of blockchain technology can be predicted using the unified theory of acceptance and use of technology model (UTAUT). This model developed by Venkatesh et al. (2003) served as the primary framework. The survey was distributed to students and faculty of a midsize university and IT professionals in several organizations in the Northeast region of the United States, yielding 127 usable survey responses. Results show that perceived operational usefulness has a positive influence on blockchain use, as well as perceived ease of use. Demographics also indicate the potential for growth in blockchain acceptance, including younger generations and IT professionals who could act as early adoption agent

An Overview on Smart Contracts: Challenges, Advances and Platforms

Smart contract technology is reshaping conventional industry and business processes. Being embedded in blockchains, smart contracts enable the contractual terms of an agreement to be enforced automatically without the intervention of a trusted third party. As a result, smart contracts can cut down administration and save services costs, improve the efficiency of business processes and reduce the risks. Although smart contracts are promising to drive the new wave of innovation in business processes, there are a number of challenges to be tackled. This paper presents a survey on smart contracts. We first introduce blockchains and smart contracts. We then present the challenges in smart contracts as well as recent technical advances. We also compare typical smart contract platforms and give a categorization of smart contract applications along with some representative examples.

III. SYSTEM ANALYSIS

3.1 Existing System

Existing system based on consortium block chain technology. They used a secret sharing scheme. It can validate the digital certificate to protect the user's information and also the property of the user. The digital certificate revocation lists have collaborated among the CA The trust and reliable CRL(Certificate Revocation List)are more compared with the traditional system. If the user wants to verify the certificate, they only need to decrypt the signature with the public key. And the result will be compared with the hash operation of the original message. If the result is consistent, it proved that the digital certificate not tampered. But there is a false sense of security.

Disadvantage of Existing System:

1. Security is less.

3.2 PROPOSED SYSTEM

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. The chaotic algorithm used for generating the hash value. Each block consists of the hash value, timestamp, and hash value of the previous block. These blocks are linked together in the form of blockchain. The institution registers the student details in our interface (application) by providing details like name, email id and these are stored in the database. The certificate issued by the registrar is stored in the application and they form a blockchain. The employer or verifier can validate the certificate by entering the student details. By using the un-modifiable property of blockchain provide more security. Confidentiality is transparent with each transaction visible to all the peers. Our

application runs in offline mode. The certificate is validated rapidly. Provide accurate and reliable information.

Advantages:

1. Security is more.

Modules:

1) Save Certificate with Digital Signature
2) Verify Certificate

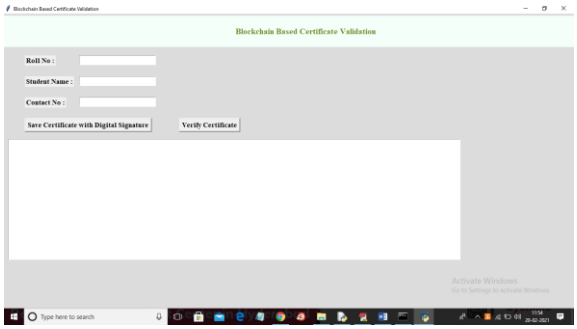
Modules Description

Save Certificate with Digital Signature: Using this module admin user can upload student details and student academic certificate and then application convert certificate into digital signature and then signature and other student details will be saved in Blockchain database.

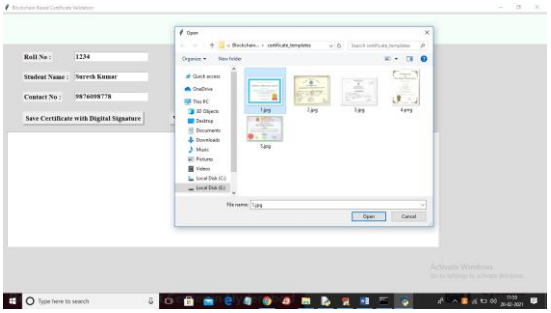
Verify Certificate: In this module verifier or companies or admin will take certificate from student and then upload to application and then application will convert certificate into digital signature and this digital signature will get checked/verified at Blockchain database and if matched found then Blockchain will retrieve all student details and display to verifier and if match not found then this certificate will be consider as fake or forge.

IV. SCREENSHOTS

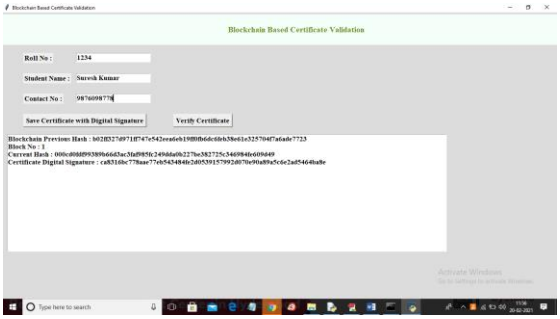
To run code double click on 'run.bat' file to get below screen



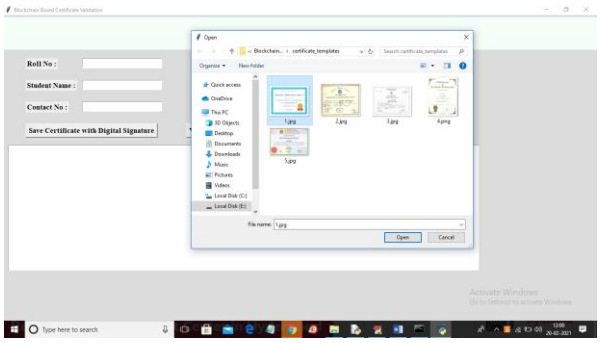
In above screen enter student details and then click on 'Save Certificate with Digital Signature' button to convert certificate into digital signature and then saved in Blockchain



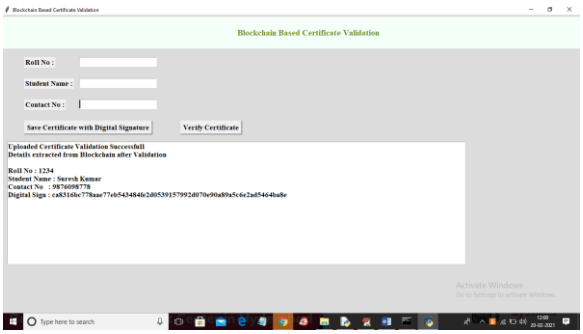
In above screen entered some student details and then click on 'Save Certificate with Digital Signature' button and then selecting and uploading '1.jpg' file and then click on 'Open' button to get below screen



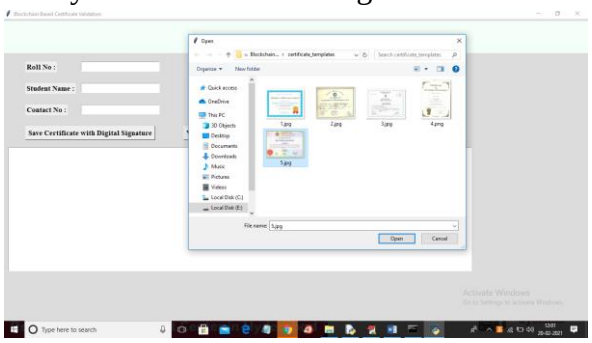
In above screen we can see Blockchain generated previous hash with block no 1 and its current hash and then keep on generating new blocks with each certificate upload and while running you can see that previous hash of new record will get matched with current hash of old record and this matched hash code proof that Blockchain verify old and new hash code before storing new block to confirm data is not altered. So above details stored at Blockchain and now verifier can click on 'Verify Certificate' button and upload same or other images to get below result



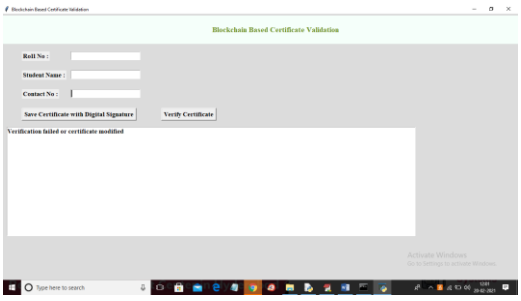
In above screen selecting and uploading '1.jpg' file and then click on 'Open' button to get below result



In above screen we uploaded same and correct image so application matched digital signature and then retrieve details from Blockchain and now try with some other image



In above screen selecting and uploading '5.jpg' file and then click on 'Open' button to get below result



In above screen verification got failed as uploaded certificate not matched with stored certificates in Blockchain.

Similarly you can upload any other certificate and convert them to digital signature

V. 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. Using the proposed blockchain-based system reduces the likelihood of certificate forgery. The process of certificate application and automated certificate granting are open and transparent in the system. Companies or organizations can thus inquire for information on any certificate from the system. In conclusion, thesystem assures information accuracy and security.

REFERENCES

[1] Tengyu Yu, Blockchain operation principle analysis:5 key technologies, iThome, https://www.ithome.com.tw/news/105374

[2] JingyuanGao, 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/bitcoinether-litecoin-ripple-differences-betweencryptocurrencies

[3] Smart contractswhitepaper, 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/b0499306-1905-4531-888a2bc4c1ddb391/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 EthereumBlockchain",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] ZhenzhiQiu, "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 developmentstatus and trends, http://nmarlt.pixnet.net/blog/post/65851006-%E5%85%A8%E7%90%83%E5%8D%80%E5%A1%8A%E9%8F%88%E7%99%BC%E5%B1%95%E7%8F%BE%E6 %B3%81%E8%88%87%E8%B6%A8%E5%8B%A 2

[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, IntroducingEthereum and Solidity, https://www.apress.com/br/book/9781484225349

[12] Jan Xie, Serpent GitHub, https://github.com/ethereum/wiki/wiki/%5B%E4%B 8% AD%E6%96%87%5DSerpent% E6%8C%87%E5%8D %97 Solidity , https://solidity.readthedocs.io/en/latest/index.html