ISSN: 2321-2152

IJMECE

International Journal of modern electronics and communication engineering

E-Mail
editor.ijmece@gmail.com
editor@ijmece.com

www.ijmece.com

ISSN2321-2152
www.ijmece .com
Vol 9 Issue 4 Nov 2021

BLOCKCHAIN BASED CERTIFICATE VALIDATION

Dr. B. Hari Krishna

ABSTRACT:

In this project to secure academic certificate and for accurate management and to avoid forge certificate we are converting all certificates into digital signatures and this digital signatures will be stored in Blockchain server as this Blockchain server support tamper proof data storage and nobody can hack or alter its data and if by an chance if its data alter then verification get failed at next block storage and user may get intimation about data alter. In Blockchain technology same transaction data stored at multiple server with hash code verification and if data alter at one server then it will detected from other server as for same data hash code will get different. For example in Blockchain technology data will be stored at multiple servers and if malicious users alter data at one server then its hash code will get changed in one server and other servers left unchanged and this changed hash code will be detected at verification time and future malicious user changes can be prevented. In Blockchain each data will be stored by verifying old hash codes and if old hash codes remain unchanged then data will be consider as original and unchanged and then new transaction data will be appended to Blockchain as new block. For each new data storage all blocks hash code will be verified.

Keywords:Blockchain, Server, tamper, ML.

1. INTRODUCTION:

The project consists in designing and implementing the system which covered the above solutions. The project also involves a comprehensive evaluation of the system security, and the assessment outcomes provide compelling evidence to prove that implementation is practical, reliable, secured, which might give some hints of important architectural considerations about the security attributes of other blockchain-based systems. In this section, we discuss the implementation from the point of view of system architecture, database architecture. The system architecture and database architecture show how the system is designed from the engineering point of view.The issuing applications are responsible for the main business logic which include the certificates applying, examining, signing and issuing. The issuing applications are designed to merge the hash of the certificate in a Merkle tree and send the Merkle root to Blockchain amidst signing by the majority of community members. Also, the issuing applications involved the revocation of certificate. The issuing applications are responsible for the main business

Associate Professor, Dept. of CSE,
Malla Reddy Engineering College (Autonomous),
Secunderabad, Telangana State

logic which includes the applying for, examining, signing and issuing of the certificates. The issuing applications are designed to merge the hash of the certificate with a Merkle tree and send the Merkle root to the Blockchain. Also, the issuing applications deal with the revocations of certificates.

The verification application focuses on checking the authenticity and integrity of the certificates that have been issued. It includes two main components: a web-based page and an Android-based application. They use the same mechanism, and fetch the transaction message through the blockchain API and compare the transaction message with the verification data from the receipt. The mechanism can be briefly described in the following way: check the authentication code is valid; check the hash with the local certificate; confirm the hash is in the Merkle tree; ensure the Merkle root is in the blockchain; verify the certificate has not been revoked; validate the expired date of the certificate. Also, it has to be mentioned that for the convenience of sharing the certificates, the Android-based application allows for verification of the documents by scanning the QR code directly. The blockchain acts as the infrastructure of trust and a distributed database for saving the authentication data. Typically, the authentication data consist of the Merkle root generated using hashed data from thousands of certificates. The MongoDB is employed as our database since the MongoDB successfully manages JSON-based certificates and provides high availability and scalability. 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— Bitcoin, Ether, and Ripple [2]—the value of which has surged recently. People are beginning to pay attention to blockchain, the backbone technology of these revolutionary currencies. Blockchain features a decentralized and incorruptible database that has high potential for a diverse range of uses

Blockchain 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 [1]. 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.

2. LITERATURE SURVEY

EXISTING SYSTEM

The certificate are stored in centralized manner and verified manually, so it takes too much time to verify. There is no safety to the certificate that are given to any private sectors (banks).But,thedatas may be changed, deleted or modified. Certificates are easily hacked and make duplicate of that certificate. Students bring their certificates on interview places. There is no security for certificates.

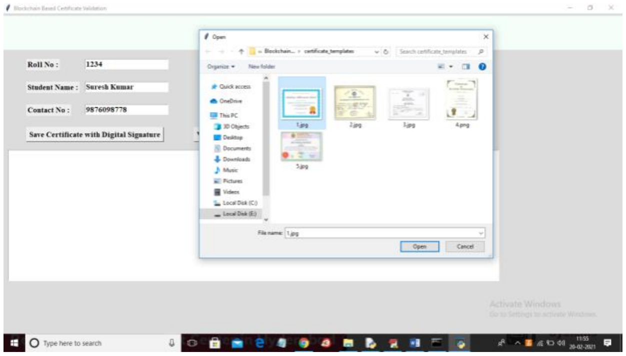
PROPOSED SYSTEM

In this study, a blockchain certificate system was developed based on relevant technology. The system's application was programmed on the Ethereum platform and is run by the EVM. In the system, three groups of users are involved, Schools or certification units grant certificates, have access to the system, and can browse the system database. When students fulfilled certain requirements, the authorities grant a certificate through the system. After the students have received their certificate, they are able to inquire about any certificate they have gained. The service.

3. METHODOLOGY

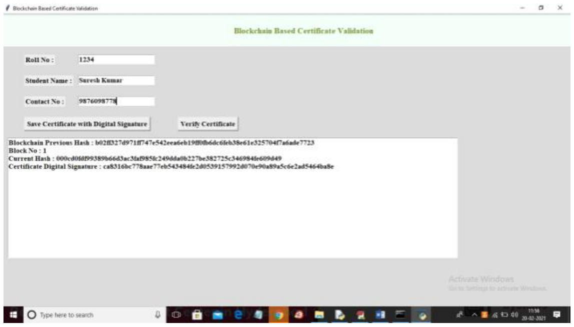
System Design In this study, a blockchain certificate system was developed based on relevant technology. The system's application was programmed on the Ethereum platform and is run by the EVM. In the system, three groups of users are involved, Schools or certification units grant certificates, have access to the system, and can browse the system database. When students fulfilled certain requirements, the authorities grant a certificate through the system. After the students have received their certificate, they are able to inquire about any certificate they have gained. The service Process Blockchain is a decentralized distributed database. The working processes of the system developed in this study are as follows: Schools grant a degree certificate and enter the student's data into the system. Next, the system automatically records the serial number of the student in a blockchain. The certificate system verifies all the data. Instead of sending conventional hard copies, schools grant e-certificates containing a quick response (QR) code to the graduates whose data have been successfully verified. Each graduate also receives an inquiry number and electronic file of their certificate. When applying for a job, a graduate simply sends the serial number or e-certificate with a QR code to the target companies. The companies send inquiries to the system and are informed if the serial numbers are validated. The QR code enables them to recognize if the certificate has been tampered with or forged.

Working:



Roll No : 1234
Student Name : Suresh Kumar
Contact No : 9876098778
Save Certificate with Digital Signature
File name: 1.jpg

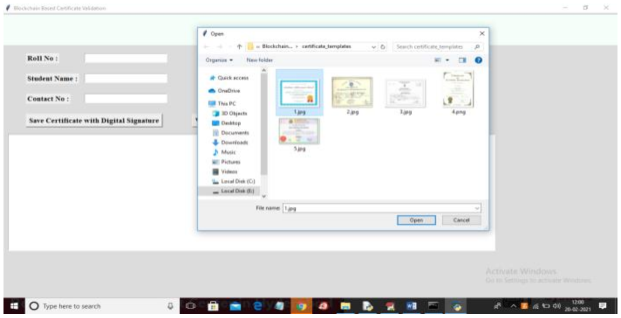
In above screen entered some student details and then click on ‘Save Certificate with Digital Signature’ button and then selecting and uploading ‘1.jpg’ file and then click on ‘Open’ button to get below screen


Blockchain Based Certificate Validation
Save Certificate with Digital Signature
Verify Certificate
Type here to search

Roll No : 1234
Student Name : Suresh Kumar
Contact No : 9876098778

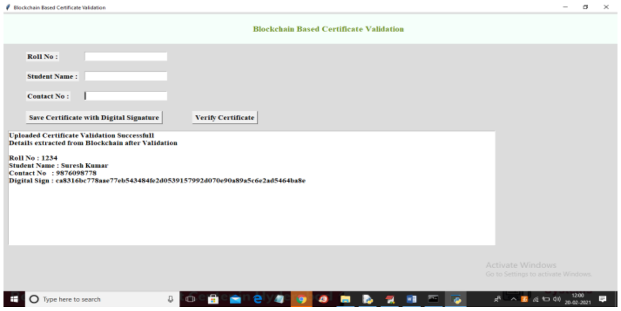
```
Blockchain Previous Hash : b02ff327d971ff747e542eea6eb19ff0fb6dc6feb38e61e325704f7a6ade7723
Block No : 1
Current Hash : 000cd0fdf99389b66d3ac3faf985fc249dda0b227be382725c346984fe609d49
Certificate Digital Signature : ca8316bc778aae77eb543484fe2d0539157992d070e90a89a5c6e2ad5464ba8e
```

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



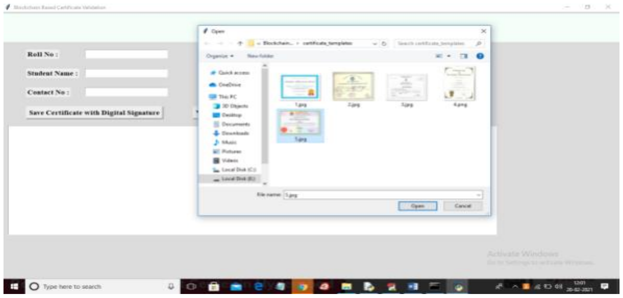
File name: 1.jpg

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


Blockchain Based Certificate Validation
Roll No :
Student Name :
Contact No :
Save Certificate with Digital Signature
Verify Certificate
Type here to search

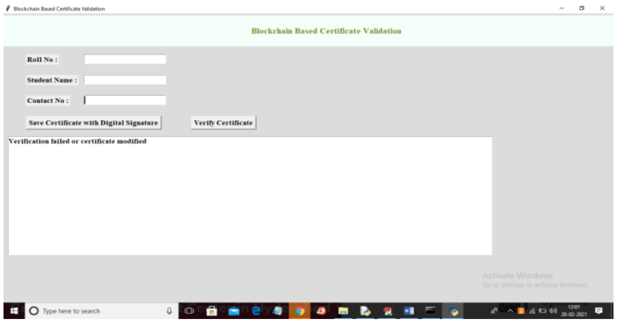
```
Uploaded Certificate Validation Successfull
Details extracted from Blockchain after Validation

Roll No : 1234
Student Name : Suresh Kumar
Contact No   : 9876098778
Digital Sign : ca8316bc778aae77eb543484fe2d0539157992d070e90a89a5c6e2ad5464ba8e
```

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



File name: 5.jpg

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


Blockchain Based Certificate Validation
Roll No :
Student Name :
Contact No :
Save Certificate with Digital Signature
Verify Certificate
Activate Windows
Go to Settings to activate Windows.
Type here to search
12:01
20-02-2021

Blockchain Based Certificate Validation

Verification failed or certificate modified

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.

CONCLUSION

In June 2016, the MIT media lab released their blockchain-based credential system which is more secure, more reliable and harder to forge, in contrast to existing technologies that based on the third party arbitration. However, there are some serious authentication defects and vulnerable revocation mechanism which limits the prevalence and application of the project. In our project, to solve these problems and make its concept more practical, we proposed and designed a set of innovative cryptographic protocols which includes multi-signature, BTC- address-state-based revocation mechanism and trusted federated identity

Among these protocols, the multi-signature scheme most notably increases the difficulty of forging owing to the fact that each issuing progress is obliged to be signed by the majority of the academic committee members. Besides, it enhances the safety of the private keys storing for the reasons that the private keys are possessed by separated devices and people. Besides, BTC-address-based revocation mechanism improved the stability of the certificate revocation because BTC address is accessible and stable at any time. Moreover, this approach reduced the failure probability of revocation, because the cancellation process adheres the same the multi-signature algorithm, alike, involving several people. Trusted federated identity innovatively proved the authenticity of the certificate through the trusted path and federated identity. What's more, the protocol of our project can be used in other related realms such as digital right protecting and contract proof. Case in point, our protocol enables the two companies to attach their contract onto the block chain with multisignature, which is different from the traditional third party-based work mode and dispel the worries of forging credentials.

Moreover, we implemented a blockchain-based certificate system, which embraced all the above protocols, by utilizing Java and JavaScript. This system has remedied the defect in Blockcerts to a certain extent, which makes the theory of blockchain-based certificate more practicable. Eventually, we conducted a series of security assessment from the perspective of operational safety, data security, network security and protocol security. The assessment outcomes provide compelling evidence that system is secured enough to meet the enterprise application standards.

Lastly, there are some limitations remained to be discussed, albeit, these considerations fall outside the scope of this paper: Our project is based on the Bitcoin blockchain, the maintenance of which relies on thousands of participants in the cryptocurrency ecosystem. Admittedly, it is imprudent to assume that the Bitcoin would work well continuously in the future because myriad types of stakeholders influence blockchain ecosystem or business model. In the years to come, we will adopt multiple blockchain sources such as Hyperledger and Ethereum to eliminate the factors of instability.

REFERANCES

[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-li tecoin-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/b0499306-1905-4531-888a-2bc4c1ddb391/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 development status and trends,

[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.