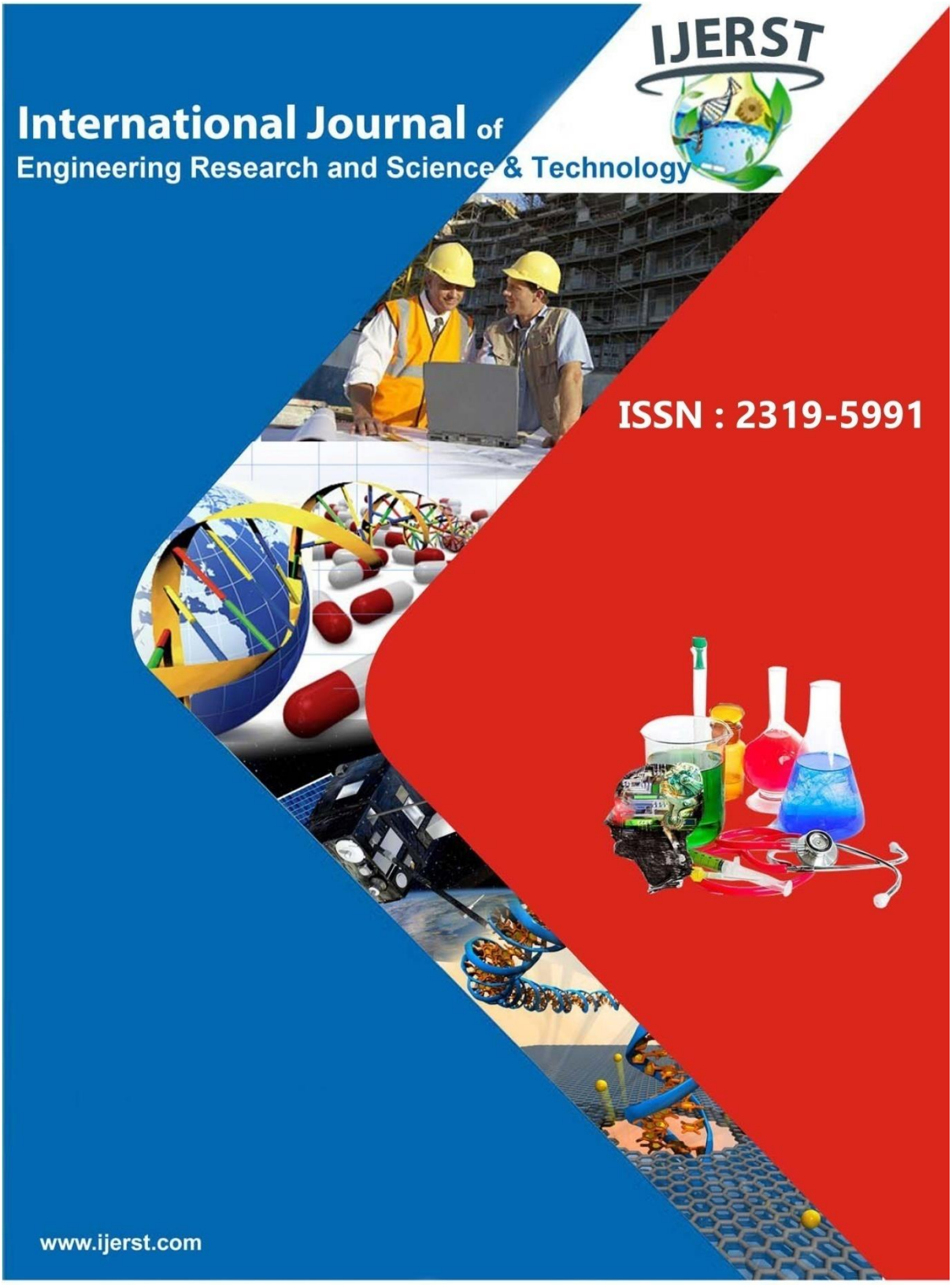


Email: editor@ijerst.com or editor.ijerst@gmail.com

International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com

Vol. 10, Issuse.3,July 2022

BLOCKCHAIN BASED CERTIFICATE VALIDATION

BOOSA HARINI1, KONDAKINDI SRI HARSHA2, BANDARI VINOD DIVYA3, S PRAVALIKA4

ABSTRACT:

In this project, we are converting all certificates into digital signatures in order to secure academic certificates, for accurate management, and to prevent certificate forgery. These digital signatures will be stored in a blockchain server because this blockchain server supports tamper-proof data storage, meaning no one can hack or alter its data. If by chance, if its data alter, verification will fail at the next block storage, and the user may be informed about the data alter. Similar transaction data is saved across many servers in blockchain technology with hash code verification. If data is altered on one server, it will be discovered on the other server since the hash code will change. For instance, in Blockchain technology, data is stored across multiple servers. If malicious users change data at one server, the hash code will change there while remaining unchanged on the other servers. This changed hash code will be discovered during verification, preventing further malicious user changes. Each piece of data in a blockchain is saved by comparing it to older hash codes; if the older hash codes are unmodified, the data is regarded as original and unaltered, and a new block of transaction data is added to the blockchain. Every new block of data storage will have its hash code validated.

Keywords: ML, server, tamper, and blockchain.

1.INTRODUCTION:

The system that addressed the aforementioned problems was designed and put into operation as part of the project. The project also includes a thorough examination of the system security, and the assessment results provide persuasive proof that the implementation is workable, dependable, and secure, which may provide some suggestions of significant architectural concerns for other blockchain-based systems' security features. The implementation is covered in this part from the standpoints of system and database architecture. The database architecture and system architecture both demonstrate how the system was created from an engineering standpoint.The basic business logic, which includes the issuing apps, is in charge ofapplying, evaluating, signing, and issuing certificates. The certificate's hash will be combined in a Merkle tree by the issuing apps, which will then submit the Merkle root to Blockchain while the majority of the community members sign it. The cancellation of certificates was also a part of the applications for issue. The primary business logic, including applying for, reviewing, signing, and issuing certificates, is handled by the issuing apps. The

1,2, 3, 4 UG Student, Department of CSE, NARSIMHA REDDY ENGINEERING COLLEGE, Maisammaguda, Kompally, Secunderabad, Telangana India. 500100

certificate's hash and a Merkle tree are combined by the issuing software, which then sends the Merkle root to the Blockchain. The applications for granting certificates also include the cancellation of certifications. The verification application focuses on examining the validity and reliability of the given certifications. There are two primary parts to it: an Android application and a web website. They use the same approach and get the transaction message through the blockchain API before comparing it to the verification information on the receipt. The mechanism can be summed up as follows: confirm the authenticity of the authentication code; validate the hash against the local certificate; confirm the hash is in the Merkle tree; confirm the Merkle root is in the blockchain; confirm the certificate has not been revoked; and confirm the certificate's expiration date. Additionally, it must be noted that for

The Android-based application makes it simple to share certificates and enables for instant document verification by scanning the QR code. The blockchain serves as a distributed database for storing the authentication data as well as the architecture of trust. The Merkle root, which is created using hashed information from hundreds of certificates, often makes up the authentication data. Since the MongoDB effectively supports JSON-based certificates and offers high availability and scalability, the MongoDB is used as our database. The way that people live has changed as a result of developments in information technology, the widespread use of the Internet, and the widespread use of mobile devices. Digital coins known as virtual money, which were first created for usage online, are now widely used offline. The ease of the Internet has led to the growth of several virtual currencies, the most well-known of which are Bitcoin, Ether, and Ripple [2], the value of which has lately increased. The blockchain, the core technology behind these innovative currencies, is starting to attract attention. Blockchain provides a decentralized, unchangeable database with great potential for a variety of purposes.

Blockchain is a decentralized database that's often used to record various transactions. The transaction is added to a block that already contains records of numerous transactions after consensus among the various nodes has been obtained.

The hash value of a block's most recent connection counterpart is included in each block. A blockchain is created when all the blocks are linked to one another [1]. Data are decentralized because they are dispersed across several nodes (the distributed data storage). As a result, the nodes jointly maintain the database. A block in a blockchain is only considered genuine when it has been confirmed by several parties.

2. EXISTING LITERATURE SURVEY SYSTEM

It takes too long to validate since the certificate is manually checked and kept in a centralized location. The certificates issued to any private sector are not secure (banks). However, the data may be edited, removed, or altered. It is simple to compromise certificates and create copies of them. On the day of the interview, students bring their credentials. Certificates lack any security.

SUGGESTIVE SYSTEM

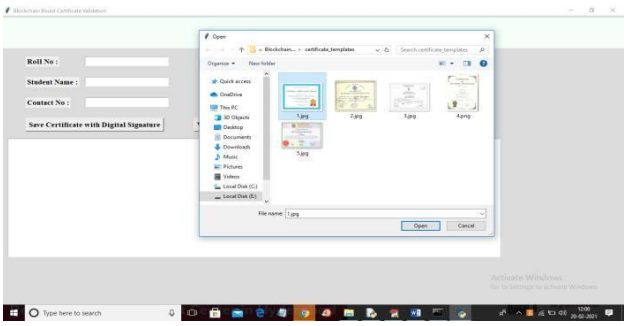
Based on the technologies used in this research, a blockchain certificate system was created. The system's application is operated by the EVM and was created on the Ethereum platform. Schools or certification units give certifications, have access to the system, and may explore the system database. These three kinds of users are participating in the system. when pupils

the necessary criteria, the authorities issue a certificate through the system. The students may ask questions concerning any certificates they have obtained after receiving their certificate. the offering.

3. METHODOLOGY

Creating Systems Based on the technologies used in this research, a blockchain certificate system was created. The system's application is

operated by the EVM and was created on the Ethereum platform. Three user groups are present in the system: Certificates are issued by schools or certifying agencies, who also have access to the system and may search its database. The system is used by the authorities to issue certificates to students after they have met certain requirements. The students may ask questions concerning any certificates they have obtained after receiving their certificate. The program Process Blockchain is a distributed database that is not centralized. The system created in this research operates according to the following processes: Schools award degree certificates and input student information into the database. The student's serial number is then automatically recorded by the system on a blockchain. All of the data is verified by the certificate system. Schools provide graduates

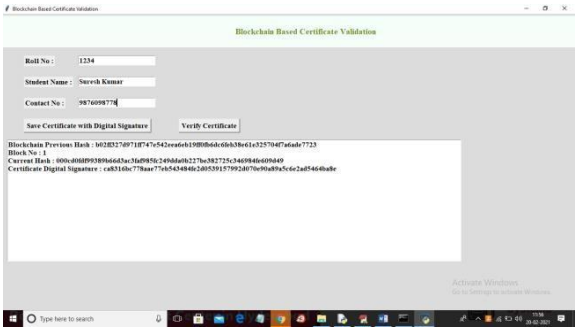


whose data has been verified with electronic certificates that include a quick response (QR) code rather than traditional physical copies.

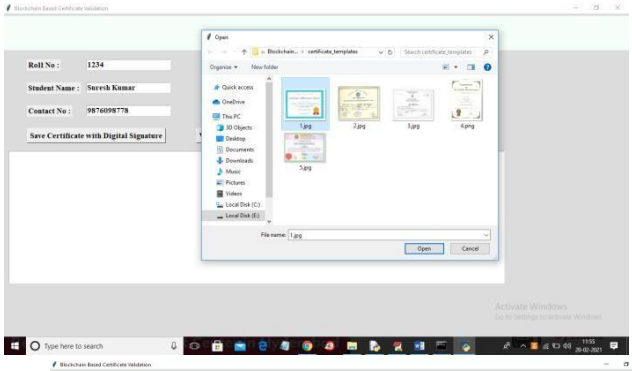
successful confirmation A enquiry number and an electronic copy of their certificate are also given to each graduate. A graduate may apply for a job by simply sending the serial number or an electronic certificate with a QR code to the desired employers. Companies submit requests to the system, and if the serial numbers are verified, they get notifications. They can determine if the certificate has been tampered with or falsified thanks to the QR code.

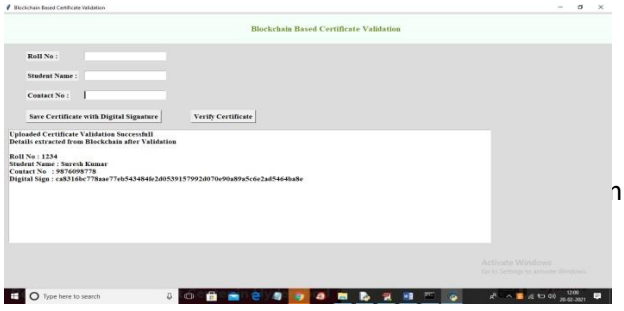
Working:

Entering some student information on the top screen, clicking "Save Certificate with Digital Signature," choosing and uploading "1.jpg," and then clicking "Open" will bring up the screen below.



The previous hash of the new record will match the current hash of the old record as you can see in the screenshot above. This matching hash code proves that Blockchain verifies the old and new hash codes before storing new blocks to ensure data is not altered. The blockchain keeps on generating new blocks with each certificate upload. Therefore, the information above was recorded on a blockchain, and the verifier may now click the "Verify Certificate" button and submit the same or other photographs to get the following result.

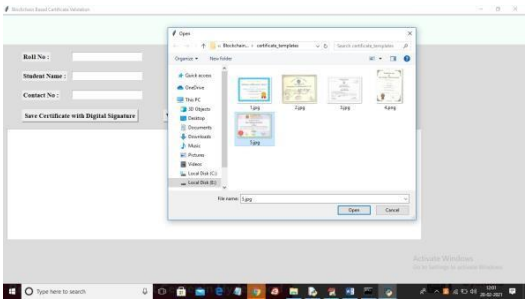


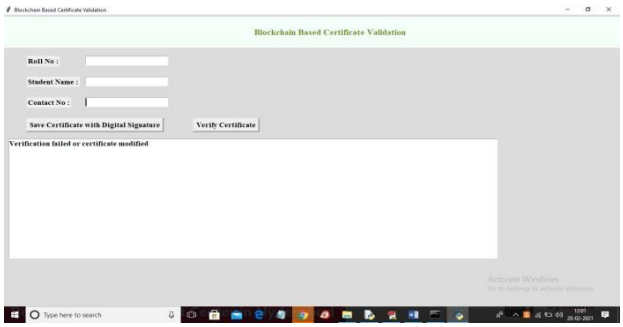


Selecting "1.jpg" from the preceding screen, uploading it, and then clicking "Open" will provide the following result

The program matched the digital signature since we submitted the identical and accurate picture on the screen above.

then get information from Blockchain, and last test with a different picture.





Selecting "5.jpg" from the preceding screen, uploading it, and then clicking "Open" will provide the following result.

Verification failed on the screen above because the submitted certificate did not match the stored certificates in the blockchain. You may upload any other certificate and convert it to a digital signature in a similar manner.

CONCLUSION

In contrast to current solutions that rely on third party arbitration, the MIT Media Lab published its blockchain-based credential system in June 2016. It is more secure, more dependable, and difficult to fabricate. However, there are several significant authentication flaws and weak points.

revocation mechanism that restricts the project's use and adoption. In our project, we developed and constructed a series of novel cryptographic protocols, including multi-signature, BTC-address-state-based revocation mechanism, and trustworthy federated identification, to overcome these issues and make its idea more workable. Since each issuing process must be signed by the majority of the academic committee members, the multi-signature method among these protocols significantly enhances the difficulty of forging. Additionally, since the private keys are held by various devices and persons, it improves the security of the private key storage. Additionally, the stability of the certificate revocation was increased by the BTC-address-based revocation process since BTC addresses are always available and reliable. Additionally, this strategy decreased the likelihood that revocation would fail since the cancellation procedure used the same multi-signature technique that included several signatories. Through the trusted path and federated identity, trustworthy federated identity creatively demonstrated the validity of the certificate. Additionally, the protocol of our study may be used to other relevant fields like contract proofing and digital right protection. For instance, using our protocol, the two businesses may link their contract to the block.chain with multisignature, which differs from the conventional third party-based work mode and allays concerns about credentials forgery.

Additionally, we used Java and JavaScript to develop a blockchain-based certificate system that included all of the aforementioned protocols. This solution has partially fixed the flaw in Blockcerts, making the principle of a blockchain-based certificate more workable. Finally, we carried out a number of security evaluations from the angles of operational safety, data security, network security, and protocol security. The results of the evaluation provide convincing proof that the system is secure enough to adhere to corporate application requirements.

Last but not least, there are still certain restrictions that need to be considered, even if they are beyond the purview of this paper: Our project is built on the Bitcoin blockchain, which is supported by thousands of users across the cryptocurrency community. It is unwise to presume that the Bitcoin system will continue to function well in the future since a wide range

of stakeholders might affect the blockchain ecosystem or business model. To remove the unstable variables, we will embrace numerous blockchain sources in the next years, including Hyperledger and Ethereum.

REFERANCES

[1] Tengyu Yu, "Blockchain operating principle analysis: 5 important technologies," iThome, available at https://www.ithome.com.tw/news/105374

[2] JingyuanGao, The development of digital money! The other four sorts can't be overlooked, but Bitcoin takes the lead. Digital Age, The distinctions between cryptocurrencies are described in https://www.bnext.com.tw/article/47456/bitcoinet her-li tecoin ripple.

[3] The whitepaper on smart contracts can be found at github.com/OSELab/learning-blockchain/blob/ master/ethereum/smart-contracts.md

[4] Gong Chen, Smart Contract Development and Use, Download the document at https://www.fisc.com.tw/Upload/b0499306-1905-4531-888a-2bc4c1ddb391/TC/9005.pdf.

[5] Weiwei He, Several national junior degrees will be introduced in 2019, free from onerous auditing and issuing processes. According to iThome, https://www.ithome.com.tw/news/119252

[6] Xiuping Lin, Department of Information Engineering, National Taiwan University, Taiwan, R.O.C., "Semi-centralized Blockchain Smart Contracts: Centralized Verification and Smart Computing under Chains in the Ethereum Blockchain", 2017.

[7] Yong Shi, "Secure storage service of electronic ballot system based on block chain algorithm," Tsing Hua University, Taiwan, R.O.C., Department of Computer Science, 2017.

[8] ZhenzhiQiu, "Blockchain-based digital certificate for a painting," National Taipei University of Technology, Taiwan, R.O.C., Department of Information and Finance Management, 2017. Global Blockchain Development Status and Trends, by Weiwen Yang

[10] Benyuan He, "An Empirical Study of Online Shopping Using Blockchain Technology," Takming University of Science and Technology, Department of Distribution Management, Taiwan, R.O.C., 2017.