International Journal of Engineering Technology and Management Sciences
Website: ijetms.in Issue: 2 Volume No.8 March - April – 2024
DOI:10.46647/ijetms.2024.v08i02.022 ISSN: 2581-4621

EDUCATIONAL CERTIFICATE VERIFICATION SYSTEM USING BLOCK CHAIN

SS.Rajkumari[1], Kapa Poojitha[2], V.Jhansi[3], Chedde Meghana[4], S.Rajiya Banu[5], R.Ayesha Siddikha[6]

[1]Asst Prof, Dept of CSE, St.johns college of Engineering and Technology, Yemmiganur, AP, India
[2,3,4,5,6]UG Scholar, Dept of CSE, St.johns college of Engineering and Technology, Yemmiganur, AP, India

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 these digital signatures will be stored in Block chain server as this Block chain server support tamper proof data storage and nobody can hack or alter its data and if by a chance if its data alter then verification get failed at next block storage and user may get intimation about data alter.

In Block chain technology same transaction data stored at multiple server with hash code verification and if data alter at one server then it will be detected from other server as for same data hash code will get different. For example, in Block chain 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 Block chain each data will be stored by verifying old hash codes and if old hash codes remain unchanged then data will be considered as original and unchanged and then new transaction data will be appended to Block chain as new block. For each new data storage all blocks hash code will be verified.

1. INTRODUCTION

OVERVIEW

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 block chain-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 Block chain 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 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 Block chain. 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

DOI:10.46647/ijetms.2024.v08i02.022 ISSN: 2581-4621

application. They use the same mechanism, and fetch the transaction message through the block chain 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 block chain; 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 block chain 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 Mongo DB is employed as our database since the Mongo DB 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 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 block chain [1]. Data are distributed among various nodes (the distributed data storage) and are thus decentralized. Consequently, the nodes maintain the database together. Under block chain, a block becomes validated only once it has been verified by multiple

2.LITERATURE SURVEY:

Verification and Validation of Certificate

Using Block chain 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 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 block chain technology would be proposed. By the modifiable property of block chain, the digital certificate with anticounterfeit 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 block chain.This research also identifies the gaps and loopholes in the current block chain-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

DOI:10.46647/ijetms.2024.v08i02.022 ISSN: 2581-4621

Design And Develop Certificate Validation System Using Smart Contract

Block chain 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 block chain 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 Block chain

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 document verification is a complex domain that involves various challenging and tedious processes to authenticate. Certificate of Block chain 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 antiforge 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 block chain technology would be proposed. By the modifiable property of block chain, 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 block chain. This research also identifies the gaps and loopholes in the current block chain-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 Block chain and Overall Behavioural Analysis using QR and Smart Contract

The Main purpose of this study is to develop a theoretical framework for block chain. Our aim is to identify the barriers and main drivers of digital innovation and explore the possibilities of applications of block chain. 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.

DOI:10.46647/ijetms.2024.v08i02.022 ISSN: 2581-4621

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 block chain technology were pointed out by earlier studies. However, we have identified many unique drivers and barriers specific to the industry. Finally, the framework of block chain process developed.

Block chain 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 mark sheets, 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 block chain 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 block chain. 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 ecert 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

Block chain 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. Block chain 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 block chain technology. The main goal of this analysis was to examine the current status of block chain-based voting research and online voting systems and any related difficulties to predict future developments. This study provides a conceptual description of the intended block chain-based electronic voting application and an introduction to the fundamental structure and characteristics of the block chain in connection to electronic voting. As a consequence of this study, it was discovered that block chain systems may help solve some of the issues that now plague election systems. On the other hand, the most often mentioned issues in block chain applications are privacy protection and transaction speed. For a sustainable block chain-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 block chain 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

DOI:10.46647/ijetms.2024.v08i02.022 ISSN: 2581-4621

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 block chain 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 block chain based e-voting scheme in P2P network is proposed for essential requirements of e-voting process. To prove and verify the scheme, a block chain-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 block chain-based e-voting system can be applied to a variety of networking applications directly.

An Empirical Study of Online Shopping Using Block chain Technology

This study specifically explores whether user acceptance of block chain 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 block chain use, as well as perceived ease of use. Demographics also indicate the potential for growth in block chain 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 block chains, 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 block chains 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.

EXISTING SYSTEM VS PROPOSED SYSTEM

EXISTING SYSTEM

The certificates 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, the data 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 block chain 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

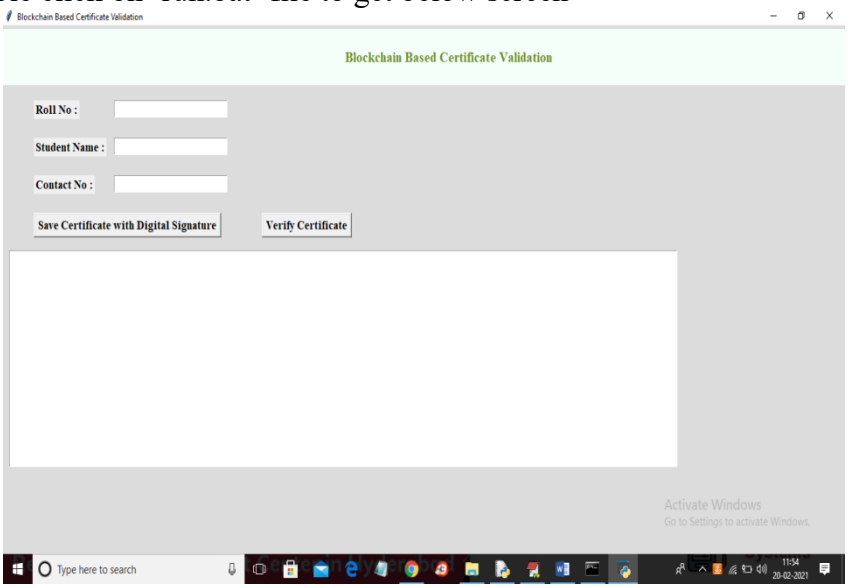
International Journal of Engineering Technology and Management Sciences
Website: ijetms.in Issue: 2 Volume No.8 March - April – 2024
DOI:10.46647/ijetms.2024.v08i02.022 ISSN: 2581-4621

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.

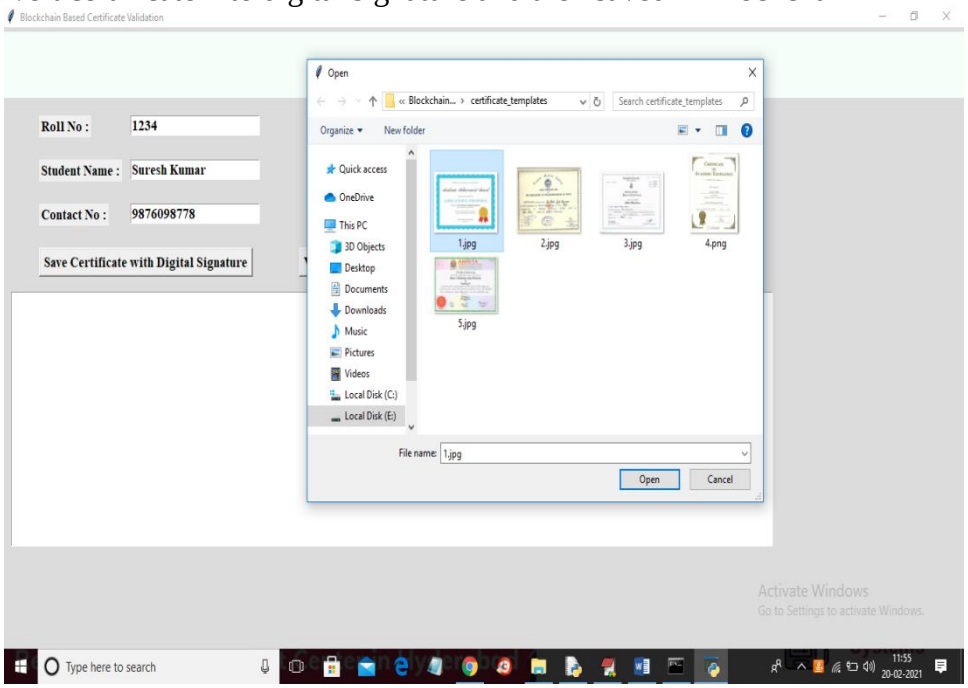
KEY WORDS:
1.DIGITAL SIGNATURE
2.SMART CONTRACT
3.DAPPS(DECENTRALISATION APPS)
4. ELECTRONIC BALLOT SYSTEM
5.EDUCATIONAL CERTIFICATES
6.SECURITY

RESULTS

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

International Journal of Engineering Technology and Management Sciences
Website: ijetms.in Issue: 2 Volume No.8 March - April – 2024
DOI:10.46647/ijetms.2024.v08i02.022 ISSN: 2581-4621

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

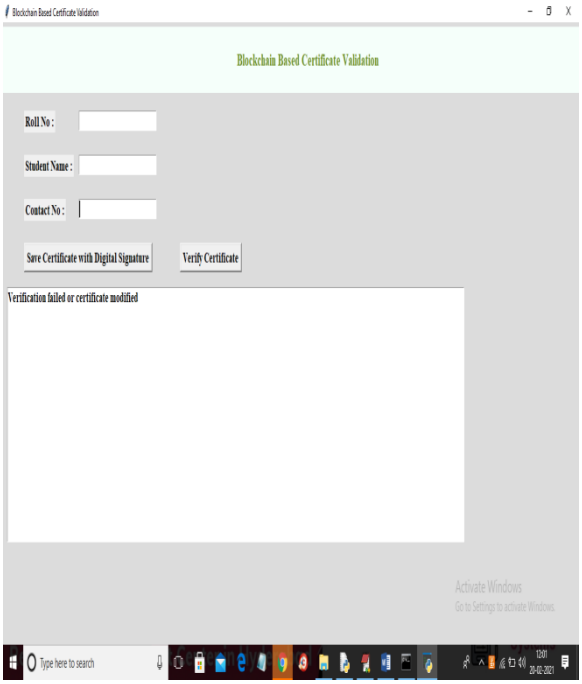
In above screen we can see Blockchain generated previous hash with block no 1 and its current hash and then keep on generating new blocks with each certificate upload and while running you can see that previous hash of new record will get matched with current hash of old record and this matched hash 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

International Journal of Engineering Technology and Management Sciences
Website: ijetms.in Issue: 2 Volume No.8 March - April – 2024
DOI:10.46647/ijetms.2024.v08i02.022 ISSN: 2581-4621

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

CONCLUSIONS

In June 2016, the MIT media lab released their block chain-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 block chain-based certificate system, which embraced all the above protocols, by utilizing Java and JavaScript. This system has remedied the defect in Block certs to a certain extent, which makes the theory of block chain-based certificate more practicable. Eventually, we conducted a series of security assessment from the perspective of operational safety,

DOI:10.46647/ijetms.2024.v08i02.022 ISSN: 2581-4621

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 block chain, 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 stake holders influence block chain ecosystem or business model. In the years to come, we will adopt multiple block chain sources such as Hyperledger and Ethereum to eliminate the factors of instability

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-li tecoin-ripple-differences-between cryptocurrencies

[3]Smart contracts whitepaper, 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 Block chain Smart Contracts: Centralized Verification and Smart Computing under Chains in the Ethereum Block chain”, 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 block chain technology”, Department of Information and Finance Management, National Taipei University of Technology, Taiwan, R.O.C., 2017.

[9] Weiwen Yang, Global block chain development status 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 Block chain Technology”, Department of Distribution Management, Takming University of Science and Technology, Taiwan, R.O.C., 2017.

[11] Chris Dannen, Introducing Ethereum 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%97Solidity
https://solidity.readthedocs.io/en/latest/index.html

International Journal of Engineering Technology and Management Sciences
Website: ijetms.in Issue: 2 Volume No.8 March - April – 2024
DOI:10.46647/ijetms.2024.v08i02.022 ISSN: 2581-4621

Mrs.S.S.Raja Kumari M.Tec., (Ph.D).
Associate Professor
CSE Department
St.Johns College of engineering and technology.
Yerrakota, Yemmiganur, Kurnool(Dist) AP.