Blockchain Based Certificate Validation

Srilatha Puli[1], Kandhi Vaman Reddy[2], Kankanala Vinay[3], Mughaisa Fatima[4]

[1]Assistant Professor, Department of CSE, Sreyas Institute of Engineering and Technology, Telangana, India
Email: srilatha.puli[at]sreyas.ac.in

[2]Department of CSE, Sreyas Institute of Engineering and Technology, Telangana, India
Email: vamanreddy12389[at]gmail.com

[3]Department of CSE, Sreyas Institute of Engineering and Technology, Telangana, India
vinnureddy.k[at]gmail.com

[4]Department of CSE, Sreyas Institute of Engineering and Technology, Telangana, India
mughaisafatima21[at]gmail.com

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 servers 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 verified.***

Keywords: Blockchain, SHA256, Digital Certificate, Hashcode, Multiple Servers

1.Introduction

Due to the lack of 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. By the unmodifiable property of blockchain, the digital certificate with anti-counterfeit and verifiability could be made. The procedure of issuing the digital certificate 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. It will provide the demand unit to verify the authenticity of the paper certificate through mobile phone scanning or website inquiries. Through the unmodifiable properties of the blockchain, the system not only enhances the credibility of various paper-based certificates, but also electronically reduces the loss risks of various types of certificates. 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.

2.Literature Survey

Tengyu Yu, Blockchain operation principle analysis: 5 key technologies, iThome, https://www.ithome.com.tw/news/105374
Jingyuan Gao, 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-between cryptocurrencies

Gong Chen, Development and Application of Smart Contracts, https://www.fisc.com.tw/Upload/b0499306-1905- 4531-888a-2bc4c1ddb391/TC/9005.pdf

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

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

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.

Zhenzhi Qiu, “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.

Weiwen Yang, Global blockchain development status and trends, http://nmarlt.pixnet.net/blog/post/65851006

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.

Chris Dannen, Introducing Ethereum and Solidity, https://www.apress.com/br/book/9781484225349
Jan Xie, Serpent GitHub, https://github.com/ethereum/wiki/wiki/%5,
https://solidity.readthedocs.io/en/latest/index.html

3.Existing System

So the problem with this cycle is that a student needs to produce all his certificates in each stage for validation. This poses a risk of losing and damaging the certificate. And it is tedious for the validator to authenticate each certificate. With such a huge population in our country, almost every year 26.3 million students graduate. It is very hard to keeptrack and validates such a huge amount of records. Due to this, an unwanted scenario rises i.e. tampering and production of fake or duplicate certificates. There are a lot of hidden agencies in our country who are running this scam behind everyone's back. Technology has moved quite forward until now. Distinguishing between a fake and an original certificate will require a lot of concentration and result in wastage of precious time.

Proposed System Configuration

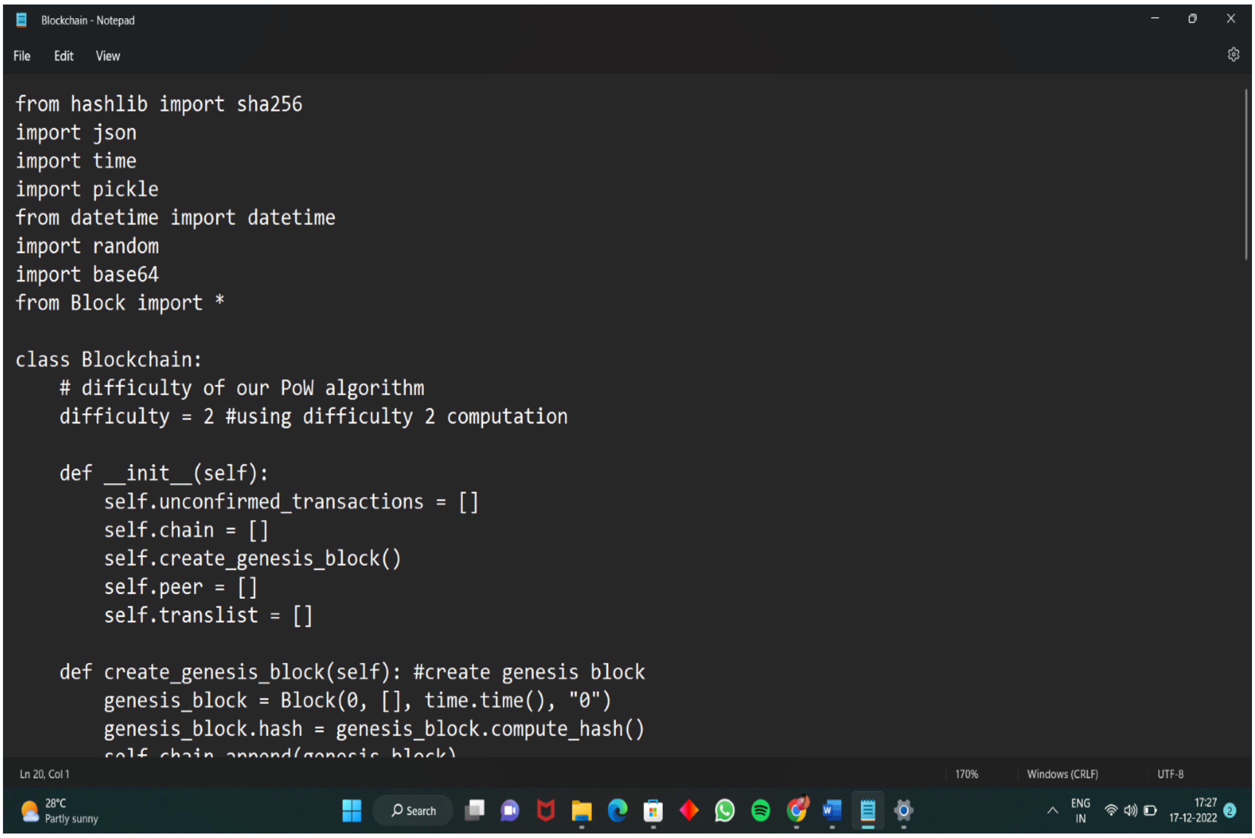
In this project to secure academic certificate and for accurate management and to avoid forge certificate we are converting all certificates into digital signatures and this digital signatures will be stored in Blockchain server as this Blockchain server support tamper proof data storage and nobody can 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.

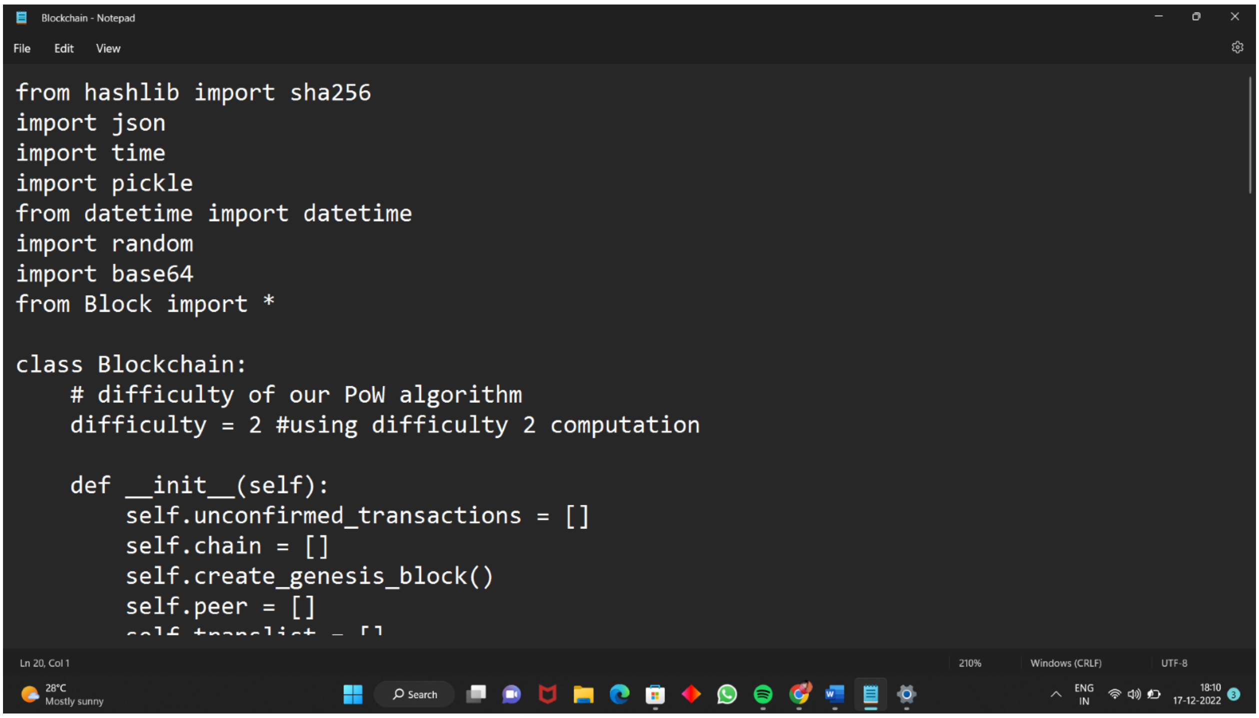
Advantages

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 change hash code will be detected at verification time and future malicious user changes can be prevented.

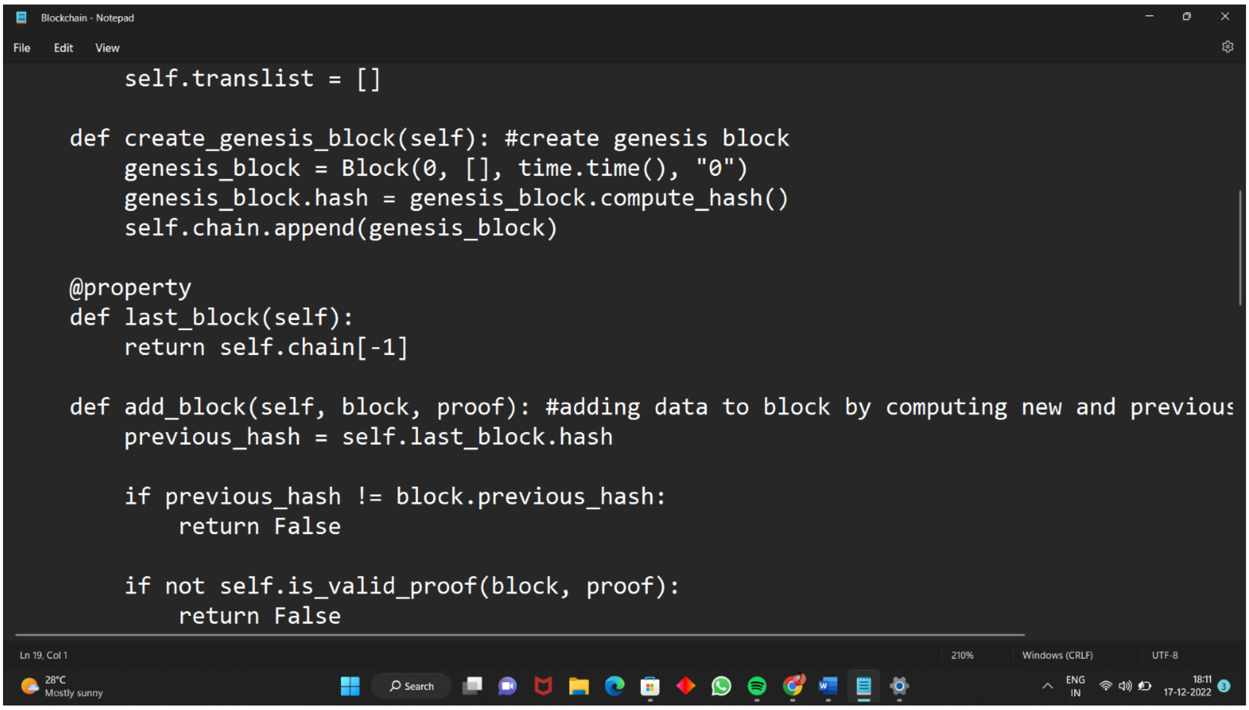
3.1 Sample Code



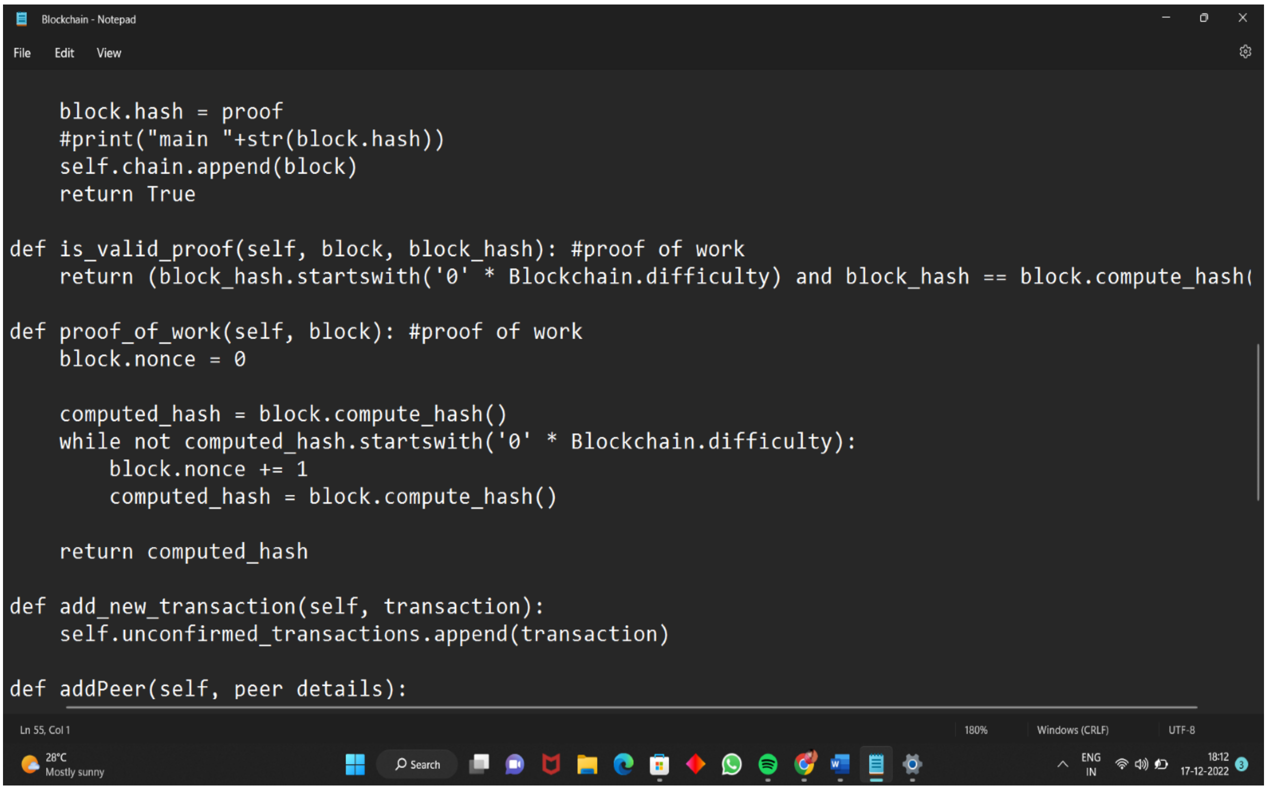
```
from hashlib import sha256
import json
import time
import pickle
from datetime import datetime
import random
import base64
from Block import *

class Blockchain:
    # difficulty of our PoW algorithm
    difficulty = 2 #using difficulty 2 computation

    def __init__(self):
        self.unconfirmed_transactions = []
        self.chain = []
        self.create_genesis_block()
        self.peer = []
        self.translist = []

    def create_genesis_block(self): #create genesis block
        genesis_block = Block(0, [], time.time(), "0")
        genesis_block.hash = genesis_block.compute_hash()
        self.chain.append(genesis_block)
```



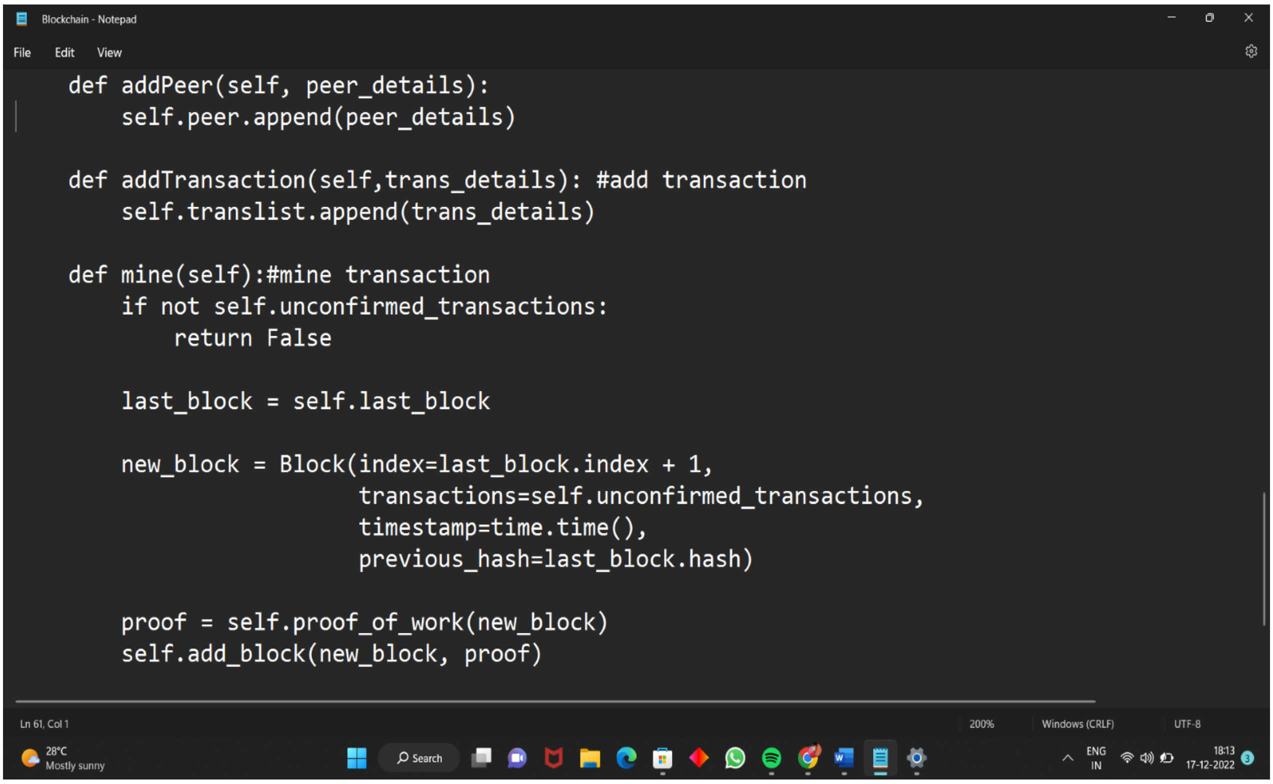
```
from hashlib import sha256
import json
import time
import pickle
from datetime import datetime
import random
import base64
from Block import *

class Blockchain:
    # difficulty of our PoW algorithm
    difficulty = 2 #using difficulty 2 computation

    def __init__(self):
        self.unconfirmed_transactions = []
        self.chain = []
        self.create_genesis_block()
        self.peer = []
        self.translist = []
```



```
        self.translist = []

    def create_genesis_block(self): #create genesis block
        genesis_block = Block(0, [], time.time(), "0")
        genesis_block.hash = genesis_block.compute_hash()
        self.chain.append(genesis_block)

    @property
    def last_block(self):
        return self.chain[-1]

    def add_block(self, block, proof): #adding data to block by computing new and previous
        previous_hash = self.last_block.hash

        if previous_hash != block.previous_hash:
            return False

        if not self.is_valid_proof(block, proof):
            return False
```



```
    block.hash = proof
    #print("main "+str(block.hash))
    self.chain.append(block)
    return True

def is_valid_proof(self, block, block_hash): #proof of work
    return (block_hash.startswith('0' * Blockchain.difficulty) and block_hash == block.compute_hash(

def proof_of_work(self, block): #proof of work
    block.nonce = 0

    computed_hash = block.compute_hash()
    while not computed_hash.startswith('0' * Blockchain.difficulty):
        block.nonce += 1
        computed_hash = block.compute_hash()

    return computed_hash

def add_new_transaction(self, transaction):
    self.unconfirmed_transactions.append(transaction)

def addPeer(self, peer details):
```



```
    def addPeer(self, peer_details):
        self.peer.append(peer_details)

    def addTransaction(self,trans_details): #add transaction
        self.translist.append(trans_details)

    def mine(self):#mine transaction
        if not self.unconfirmed_transactions:
            return False

        last_block = self.last_block

        new_block = Block(index=last_block.index + 1,
                          transactions=self.unconfirmed_transactions,
                          timestamp=time.time(),
                          previous_hash=last_block.hash)

        proof = self.proof_of_work(new_block)
        self.add_block(new_block, proof)
```

Purpose

Counterfeit academic certificates have been a longstanding issue in the academic community. Not until the Massachusetts Institute of Technology Media Lab released their project of Block-certs, a technique which is mainly implemented by conflating the hash value of local files to the blockchain but remains numerous issues, did an effective technological approach protecting authentic credential certification and reputation appear.

Based on Blockcerts, a series of cryptographic solutions are proposed to resolve the issues above, including, utilizing a multi-signature scheme to ameliorate the authentication of certificates; exerting a safe revocation mechanism to improve the reliability of certificates revocation; establishing a secure federated identification to confirm the identity of the issuing institution.

Scope

This document is the only one that describes the requirements of the system. It is meant for the use by the developers, and will also be the basis for validating the final deliver system. Any changes made to the requirements in the future will have to go through a formal change approval process. The developer is responsible for asking for clarifications, where necessary, and will not make any alternations without the permission of the client.

Implementation

- Admin will take certificate from student and then upload to application.
- Then application will convert certificate into digital signature and this digital signature will get checked/verified at Blockchain database.
- If matched found then Blockchain will retrieve all student details and display to verifier.

4.Conclusions

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.

References

[1] Srilatha Puli, A Machine Learning Model For Air Quality Prediction For Smart Cities, Design Engineering || ISSN: 0011-9342 | Year 2021-Issue: 9 | Pages: 18090-18104

[2] Srilatha Puli, Quality Risk Analysis For Sustainable Smart Water Supply Using Data Perception, International Journal of Health Sciences ISSN 2550-6978 E-ISSN 2550-696x © 2022, https://doi.org/10.53730/ijhs.v6ns5.9826, 18 June 2022

[3] Srilatha Puli, Urban Street Cleanliness, Journal of Algebraic Statistics Volume 13, No.3, 2022, P.547-552, https://publishoa.com, ISSN: 1309-3452

[4] Srilatha Puli, Self-Annihilation Ideation Detection, Neuroquantology | June 2022 | Volume 20 | Issue 6 | Page 7229-7239 | Doi: 10.14704/Nq.2022.20.6. Nq22727

[5] Srilatha Puli, Crime Analysis Using Machine Learning, YMER|| ISSN: 0044-0477, April 2022

[6] Srilatha Puli, N-Grams Assisted Youtube Spam Comment Detection, YMER || ISSN: 0044-0477, April 2022

[7] Srilatha Puli, Analysis of Brand Popularity Using Big Data And Twitter, YMER|| ISSN: 0044-0477, April 2022

[8] Srilatha Puli, Cyber Threat Detection Based On Artificial Neural Networks Using Event Profiles, The International Journal of Analytical And Experimental Modal Analysis, ISSN No: 0886-9367

[9] Srilatha Puli, Face Mask Monitoring System, The International Journal of Analytical And Experimental Modal Analysis, ISSN No: 0886-9367

[10] Srilatha Puli, Iot Based Smart Door Lock Surveillance System Using Security Sensors, Advanced Science Letters E-ISSN: 1936-7317

[11] Srilatha Puli, Safety Alerting System For Drowsy Driver, 9th International Conference On Innovations In Electronics & Communication Engineering (ICIECE-2021), Page- 40

[12] N. Swapna Suhasini, Srilatha Puli, Big Data Analytics For Malware Detection In A Virtualized Framework, Journal of Critical Reviews, ISSN: 2394-5125 Vol.7, Issue 14, July- 2020