Blockchain-based Framework for Online Entrance Examination and Score Card Verification System

Thilagavathi M[a] and Daphne Lopez[b]

A
VIT University, Assistant Professor (Sr.), India (ORCID: 0000-0003-1323-2639)
[b]VIT University, Professor, India (ORCID: 0000-0003-1452-2144)

Article History: Received: 11 January 2021; Accepted: 27 February 2021; Published online: 5 April 2021

Abstract: Entrance examinations are a means through which universities select prospective students for admission. Most of the entrance exams are conducted using pen-paper in an offline mode where the number of students appearing is also very high. The current entrance examination system with centralized servers to prone to single point of failure and faces threats with respect to leaks in question papers, copying by students during the exam, impersonation, manipulation of the answers, forging the score cards, difficulty in verifying the authenticity and reliability of score cards by the university, etc. To overcome these issues and to conduct entrance exams online in a secure manner and to make the process of verifying the score card easier, a framework based on private blockchain is proposed in this paper.

Keywords: Blockchain, smart contract, online entrance exam, education

1. Introduction

Educational institutions across the globe conduct entrance examinations to select prospective students for admission into higher studies either at the international, national or university level. Separate entrance exams are conducted for each discipline, say engineering, medical, management, etc. The entrance exams conducted at international and national levels are generally conducted by an exam board designated by the corresponding nation. The number of students appearing for each entrance exam varies from thousands to lakhs. These exams are conducted in an online or offline mode. Generally, entrance exams will be conducted in different centres across the country and centres outside the country in different national and regional languages. However, the current entrance examination system with centralized servers are prone to single point of failure and faces threats with respect to leaks in question papers, copying by students during the exam, impersonation, manipulation of the answers after the exam, manipulation of score secured and thereby forging the score cards. Also the universities find it difficult to verify the authenticity and reliability of the student’s score card. Therefore, it is essential that a mechanism that can overcome the above stated issues be devised.

Blockchain Technology that was originally found to be used in exchanging digital currencies, has started to draw interest in a wide variety of industries such as IoT (Christidis and Devetsikiotis, 2016; Conoscenti el al., 2016), healthcare (Azaria et al., 2016; Xia et al., 2017; Xia et al., (2017); Rouhani et al., 2018; Kassab et al., 2019), smart cities (Salha et al., 2019), e-governance (Elisa et al., 2018; Ayed, 2017), intelligent transport systems (Yuan and Wang, 2016; Li et al., 2018), cyber security (Bansal et al., 2020; Taylor et al., 2020), to name a few.Presently some of the universities and institutes use blockchain technology in the field of education for managing credits and issuing degree certificates. Leveraging the Blockchain technology that has gained universal attention over the last few years in a multi-stakeholder, manual and paper based scenario could help fix the issues stated above. This paper presents a framework that the exam boards/universities can use to conduct entrance exams and allow the universities verify the authenticity and reliability of the student’s score cards.

This paper is organized as follows. Section 2 outlines the blockchain technology. Section 3 outlines the related works that are currently carried out. Section 4 presents the proposed Blockchain-based Framework for Online Entrance Examination and Certification System. Section 5 presents a comparison between the proposed framework and the existing blockchain based solutions. Finally section 6 concludes the paper.

2. Background

Blockchain, the core technology behind Bitcoin (Nakamoto, 2008) has gained an extensive attention in the recent years and it has revolutionized the digital world. Blockchain is a distributed open ledger that contains data that is immutable in a secure and encrypted mode and ensures that the transactions can never be altered. The transactions are validated and grouped into blocks. The validity of the blocks is decided using a consensus mechanism – a process where the miners reach on a mutual agreement. The ledger constantly grows and thus the new blocks are appended to the end of the ledger. Each new block in the ledger holds a reference to the hash of the previous block. The blocks are replicated and synchronized across multiples peers in a peer-to-peer network. The first block of the blockchain is called the genesis block and the value of the previous hash is set to 0 meaning that it has not parent block. The genesis block is typically hardcoded (Bitcoin Wiki, 2021).

Figure 1 show the blockchain architecture and Figure 2 shows the structure of a block. Each block contains the blocker header and the block body. The block header contains the block's metadata. A metadata is a data that provides information about other data that a block comprises. The block header contains the following:

i) Block Version : Version of the software tool that is used.
ii) Merkle Tree Root Hash : All transactions are validated, hashed and added to the block. Merkle Tree data structure is used to calculate the Merkle Tree Root Hash. Each block in the chain contains the root hash value of the merkle tree. A Merkle tree is a balanced tree of hashes where interior nodes are hashes of the two child hashes, all the way up to the root hash, which is the Merkle Root. It can also be used to validate the block transactions. If there are any changes made to the transaction within the block, the Merkle Root will be invalid.
iii) Time Stamp : Represents the time the block was created.
iv) Nonce : Used in Proof-of-Work.
v) nBits : Indicates the difficulty, i.e., the target threshold of Proof-of-Work.
vi) Previous Block Hash : Contains a reference to the hash of the previous block in the chain.

The block body contains a counter indicating the total number of transactions in the block plus the transactions that are validated. The number of transactions in each block depends on the block size and the size of the transactions themselves.

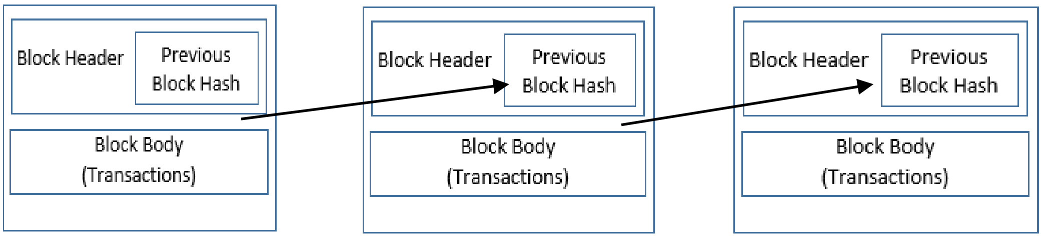

Figure 1. Blockchain Architecture

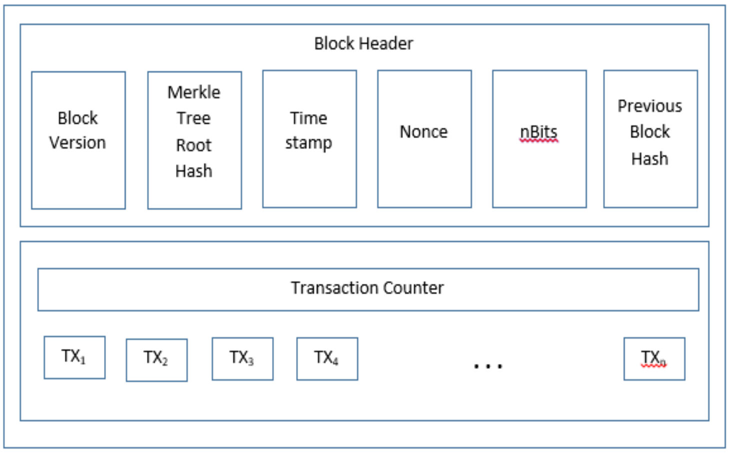

Figure 2. Structure of a Block

2.1 Features of Blockchain

Immutable – Blockchain holds a permanent record of all the transactions. A block that is added to the chain, cannot be modified (Iredale, 2020).

Enhanced Security – In addition to decentralization, another layer of protection is provided for users through cryptography (Iredale, 2020). All information on the blockchain network is cryptographically hashed. Each block in the ledger includes the hash of all the transaction data in it and the hash of the previous block. Any attempts to tamper the transaction data in a particular block will result in a different hash and that can result in breaking of chain.

Irreversible – It is one of the key feature of Blockchain. Hashing is pretty complex and it is not possible to alter or reverse it. A small change in the input will result in a completely different hash. If someone wishes to tamper the transaction data in a single block, they will have to alter all the subsequent blocks of the ledger. Trying to make changes in all the subsequent blocks of the ledger is quite impossible. And again, as the same copy of the ledger is replicated to every node on the network, trying to make changes in every node is impossible and costly.

Distributed and Decentralized – Blockchain works on a peer-to-peer network, where the nodes are connected to each other directly, without a middleman (Iredale, 2020). This feature makes the blockchain network distributed and decentralized. There is no centralized controlling authority. Hence every node on the network are authorised to make changes in the blockchain and thus it is permissionless.

Auditability – Each transaction can easily be verified and tracked.

Consensus driven – Each block in the blockchain network is verified and validated through consensus protocols. The consensus protocols specify the rubrics for validating the blocks.

Anonymity – The users interact with the blockchain through their blockchain addresses that does not reveal the actual identity.

2.2Types of Blockchain

Public Blockchain – It is a permissionless network. Hence there are no access restrictions. Anyone with an internet connection can read the transactions, send transactions to others, and take part in the consensus process. However, the data that must be retained confidential, can be encrypted (Zheng, 2017).

Private Blockchain – Also called permissioned blockchain. Only chosen nodes can join the network. It is therefore a distributed network yet centralized. It uses an access control layer to determine who can read from and write transactions to the blockchain (Zheng, 2017).

Federated or Consortium Blockchain – This type of blockchain enables only a carefully chosen group of nodes to join the network. The consensus process is controlled by known, privileged servers using a set of rules agreed to by all parties. Copies of the blockchain are only distributed among entitled participants; the network is therefore only partly decentralized(Zheng, 2017).

2.3 Consensus Protocols

As there is no centralized node in the blockchain to ensure that the ledger held by all the distributed nodes are consistent and therefore, for a blockchain network to be functional, consensus among the peers is essential as of how the blocks comprising the transactions are validated and added to the chain. The following is the list of some of the consensus protocols used: Proof-of-Work (PoW), Proof-of-Stake (PoS), Delegated-Proof-of-Stake (DPoS), Practical Byzantine Fault Tolerance (PBFT), Proof-of-Elapsed-Time (PoET), proof-of-Importance (PoI), proof-of-Activity (PoA), Proof-of-Burn (PoB), Proof-of-Space,Proof-of-Deposit (PoD), Ripple, Tendermint, etc. to mention a few. A consensus protocol specifies how a network determines which peer will prepare and add the new block (Sultan et al., 2018; Aste et al., 2017; Nguyen & Kim, 2018). The idea behind the above mentioned protocols is that the chosen node (miner) contributes something valuable and the best node is rewarded.

Proof-of-Work (PoW)

PoW consensus protocol is used in Bitcoin. The process of mining by each peer involves calculating a hash value of the block header repeatedly by changing the nonce value until the resulting hash satisfies the difficulty target that is predefined. PoW uses SHA256 for calculating the hash. The nodes that calculate the hash values are termed as miners and the process of calculating the hash is termed as mining. The miner that has calculated the hash correctly appends the block to the chain and broadcasts the newly created block to other peers on the network so that they can verify and update their ledger. The peer that wins will be rewarded appropriately. At times, there can be situations where more than one miner results in determining a hash that meets the specified difficulty target at the same time resulting in multiple valid blocks being generated simultaneously. This leads to forking problem, where there would different chains of blocks. It is implausible that two forks that are competing will generate next blocks simultaneously. With PoW, a chain that becomes longer subsequently will be treated as the authentic one. However, the drawback of PoW is that it requires significantly high computational power.

Proof-of-Stake (PoS)

It was designed to overcome the drawback of PoW. With PoS, the mining operation is replaced with an alternative approach where the miner's stake, i.e., the ownership of the amount of currency in the blockchain network will be considered as a validator for mining and creating the next valid block. It is believed that a miner with a high amount of currency is less likely to attack the network. But selecting a miner purely based on the currency balance will be quite unfair as the one with the highest balance will be dominant in the network. To overcome this problem, the PoS consensus algorithm pseudo randomly chooses the validators for block creation. However, PoS has the problem of Nothing-at-Stake.

Delegated-Proof-of-Stake (DPoS)

It is similar to PoS, miners are chosen based on their stake. The difference is that, PoS is a direct democratic whereas DPoS is representative democratic. The nodes in the network elect the miner to validate and generate the next block. DPoS is implemented in Bitshares [24].

Practical Byzantine Fault Tolerance (PBFT)

PBFT (Miguel& Barbara, 1999)consensus mechanism is deterministic, that is, the inclusion of a block in the blockchain is final. It functions in three phases – Pre-prepare, Prepare and Commit. In the Pre-prepare phase, the intended value to be committed to the blockchain is broadcasted by the leader. In the Prepare phase, the nodes in the network broadcast the values that they intend to commit. Finally, in Commit phase, for the final value to be committed, the responses from more than two thirds of the nodes must agree on the value in the Prepare phase. This mechanism requires several rounds of communication and hence scales poorly.

Proof-of-Authority

In PoA, particular miners are assigned with authority enabling them to propose new blocks.

Proof-of-Burn (PoB)

It's a proof-based algorithm. With PoB (P4Titan, 2014), the miners send their coins to a specified address to "burn" them. The miner to validate and create the next block will be the one who burns the largest amount of coins within a specified duration.

Proof-of-Space (PoS)

It's a proof-based algorithm. With Proof-of-Space (Dziembowski et al., 2015; Park et al., 2017), miners invest their money on hard disk. The algorithm generates many large datasets called plots on the hard disk. A miner with a high number of plots will have higher chances to mine a new block.

3. Related Works

Xu el al., (2017) has presented an educational certificate blockchain (ECBC) that can support low latency and increased throughput, and provides a mechanism to speed up queries. The latency reduction and increased throughput is achieved through a consensus mechanism that uses the cooperation of all the peers, so as to create blocks. A tree structure called MPT-Chain is built to provide an efficient query for a transaction with a support for historical transactions query. MPT-Chain requires less time to update and hence speed up the process of block verification. User's privacy as well is protected.

Sharples & Domingue (2016) have proposed a stable distributed record of intellectual efforts and the associated reputational reward based on the blockchain.

Disciplina (Kuvshinov et al., 2018) is a blockchain based project for education that aims at letting users to digitally store confidential data such the personal data, courses, student's grades and test results. The access to those data is provided through a uniform platform that guarantees permanence and credibility. It also allows recruiters to search for suitable candidates based on their achievements and expertise.

Bandara et al., (2018) have proposed a mechanism to validate the degree apprenticeship certifications.

Blockchain for Education (Gräther et al., 2018) is yet another blockchain platform that provides solution for issuing, validating and sharing of certificates. The system uses Ethereum and smart contracts to manage the identities of the registered certificate authorities. The SHA256 hash of the certificate, the starting and expiration date of the certificate and a status field to represent if a certificate is on hold are stored in the blockchain. Dates are represented as UNIX timestamps for future proofing. The system also uses Inter Planetary File System (IPFS) to store the profile information of certificate authorities. The use of IPFS enables saving storage on blockchain and fulfil certain data protection laws. For example, the European General Data Protection Regulation (GDPR) would object undeletable storage of any personal information on a blockchain.

Rooksby (2017) has designed and implemented an Ethereum based SmartCampus Blockchain System that helps store student's course enrolment information, grades, and final degree at the University of Glasgow. Also the top performing students in each course is rewarded using University specific cryptocurrency called the Kelvin Coin. Smart contracts were used for making reward payments. As the grades stored in the system were tamperproof and transparent, the system was highly trustworthy.

Ardnt (2018) has developed a prototype using BigChainDB blockchain to store student transcripts.

The authors have proposed EduCTX (Turkanović et al., 2018) - a blockchain-based higher education credit and grading platform based on the concept of European Credit Transfer and Accumulation System (ECTS). The prototype is implemented on the open-source ARK Blockchain platform. The EduCTX blockchain platform is intended to process, manage and control ECTX tokens as academic credits. ECTX tokens represent the credits the students has earned for the courses they have completed. The peers of the blockchain networks are the Higher Education Institutes (HEI) and users are students and potential employers. When a student completes a course, the HEI transfers an appropriate number of ECTX tokens to the students blockchain address which gets stored in the students wallet. For the purpose of security, the students are assigned with a 2-2 multi signature address by the HEI. The student can then present their blockchain address and multi signature address to the employers for verification. Delegated-Proof-of-Stake (DPoS) consensus protocol is used.

Blockcerts (MIT Media Lab, 2017), an open-source ecosystem for creating, sharing, and verifying blockchain-based educational certificates was developed by MIT Media Lab Learning Initiative in collaboration with Learning Machine, an enterprise software vendor. The educational certificates are cryptographically signed and registered on the Bitcoin blockchain. Blockcerts enables verification and validation of the owner, the issuer and the content of the certificate.

Islama et al., (2019) have proposed a blockchain based smart and secured scheme for question sharing (BSSSQS) that can be used in smart education system. The proposed scheme enables seamless sharing of question papers among the examination centres. The question papers are secured using a two-phase encryption technique and timestamp based lock.

Pee et al., (2019)in their paper has proposed an online test and management system that uses private blockchain and Ciphertext-Policy Attribute-Based Encryption (CP-ABE).

4. The proposed Blockchain-based Framework for Online Entrance Examination and Certification System

This section outlines the proposed blockchain based framework for conducting entrance exams and verifying score cards. Figure 3 depicts the proposed framework. In the proposed framework, a private blockchain network is created comprising the exam board, professors, moderators, students and universities as nodes where each node has different privilege. The professors prepare the questions, encrypt, create a hash of the encrypted questions and store the hash of the questions securely on the blockchain network. A smart contract is designed that automatically revokes the right of the professors from subsequent access to question papers to perform read, write, update or delete. The moderators will then be assigned with the privilege to read and modify the questions. The moderators would assess the quality and difficulty of the questions. Once the consensus among different moderators is reached on the final set of questions that can be used for the exam, different sets of question papers can then be created randomly. Further, the question papers undergo formatting where, if required, they can be translated into native languages and is locked from further access until the date of the exam. The final set of question papers are again encrypted and the hash of the files of stored on the blockchain network. The rights of the moderator from further access to question papers can be revoked by executing a smart contract. Then on the specified date and time, a smart contract is executed that broadcasts the question paper across the different student nodes who can then unlock the question paper using the key sent to their blockchain address and take up the exam. On completion of the exam by a student, the question number and their corresponding answers are saved as a transaction in the blockchain network. A smart contract can then be used to verify the answers and prepare a score card listing the final score and the cut-off. The universities can further verify the score cards of the students at the time of admission.

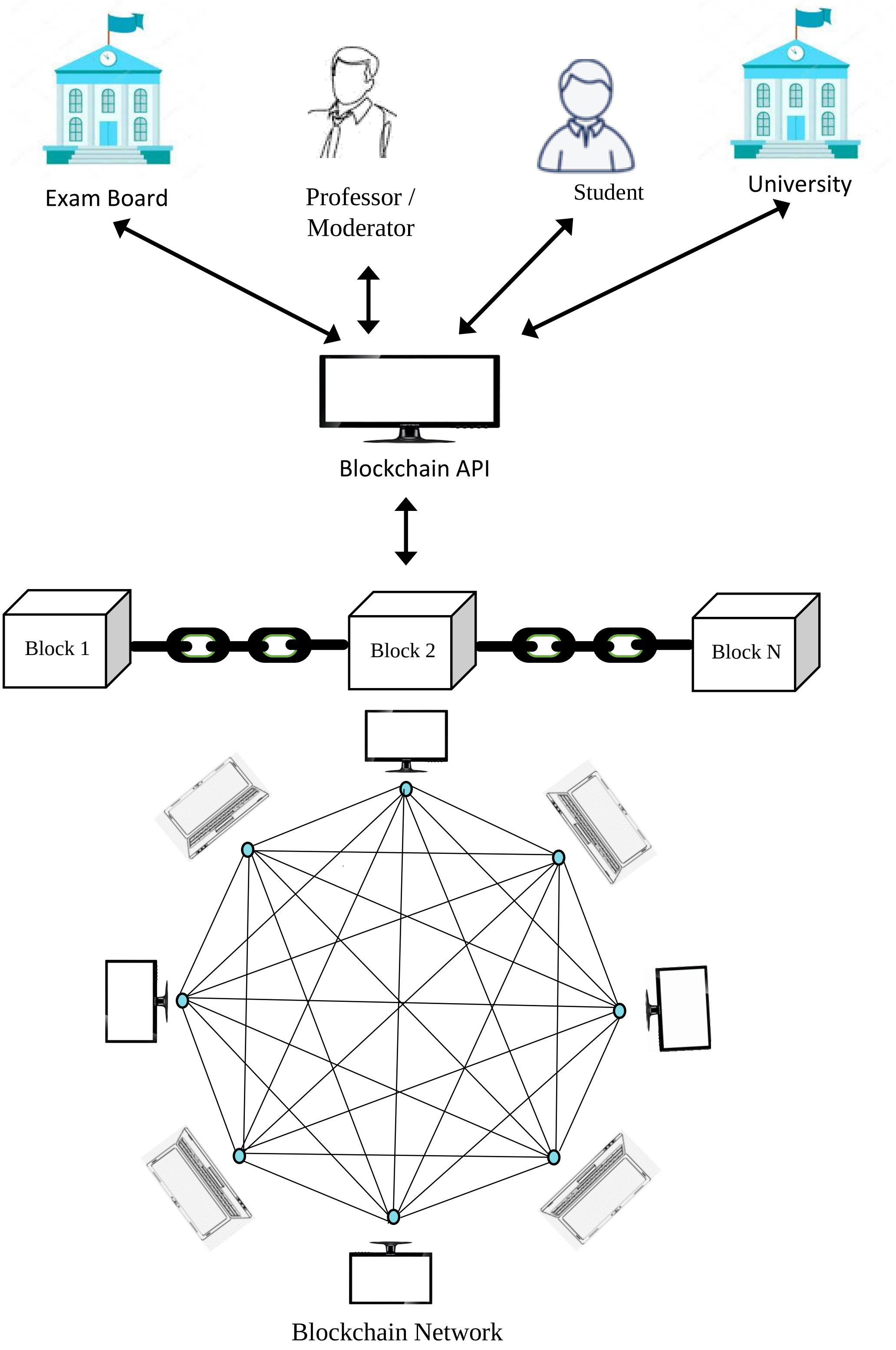

Figure 3: The Proposed Blockchain-based Framework for Online Entrance Examination and Score Card Verification System

4.1 Student Registration

The students have to register for the entrance through the API. At the time of registration, the student is expected to give an identity number that can uniquely identify them. For example, Social Security Number (SSN) in US, Aadhar Number in India, INSEE Code in France, PESEL in Poland, etc., to mention a few. This identity number can be used for instantly authenticating student's data provided at the time of registration by interfacing with corresponding verification service offered by the corresponding nation. If it doesn't find a match, the system will not register the student and will not allow them to proceed further. If valid, a unique application ID is generated. A new blockchain address is generated for the student containing public and private keys. The Exam Board (EB) sends the blockchain address containing the public and private key generated for the student along with its public key over a secure channel. Student on receiving the instructions, creates his/her blockchain wallet. The student then safely stores the ID and private key in his local device. The student then sends a transaction message to EB's blockchain address to ensure that the wallet creation was successful. The transactions are processed through blockchain network. When the transaction is confirmed, EB stores the studentID and public key of the student in its local database, confirming the student's successful wallet creation and generates the admit card which the student can use to appear in the exam. The process is summarised in Algorithm 1.

```
Algorithm 1: Student Registration
Input: Student Registration Request
Output: A newly registed student
validity ← validateStudentIdentity( );
if validity = = true
    studentID ← generateStudentID( );
    ($S_{Pub}$,$S_{Pri}$) ← generatePublicPrivateKey( );
    BlockchainAddress ← generateBlockchainAddress($S_{Pub}$,$S_{Pri}$);
    Instructions ← sendInstructions(Instructions to set blockchain wallet, $S_{Pub}$, $S_{Pri}$, $EB_{Pub}$)
    BlockchainWallet ← createBlockchainWallet($S_{Pub}$,$S_{Pri}$);
    (studentID,$S_{Pri}$) ← safelyStore(studentID, $S_{Pri}$ );
    transaction ← sendTransaction( );
    admitCard ← generateAdmitCard( );
else
    Reject Student registration
```

4.2 Professor Registration

The process of professor registration is depicted in Algorithm 2.To ensure that there are no question paper leaks from the professor's side, the question papers are not set by a single professor. So, the EB sends requests to multiple professors for setting few questions. On acceptance of the request, a unique ID for the professor is generated. A new blockchain address is generated for the professor containing public and private keys. The EB sends the blockchain address containing the public and private key generated for the professor along with its public key over a secure channel. Professor on receiving the instructions, creates his/her blockchain wallet. The professor then safely stores the ID and private key in his local device. The professor then sends a transaction message to EB's blockchain address to ensure that the wallet creation was successful. The transactions are processed through blockchain network. When the transaction is confirmed, EB stores the professorID and public key of the professor in its local database, confirming the professor's successful wallet creation.

```
Algorithm 2: Professor Registration
Input: Professor Registration
Output: A newly registered Professor

professorID ← generateProfessorID( );
($P_{Pub}$,$P_{Pri}$) ← generatePublicPrivateKey( );
BlockchainAddress ← generateBlockchainAddress($P_{Pub}$,$P_{Pri}$);
Instructions ← sendInstructions(Instructions to set blockchain wallet, $P_{Pub}$,$P_{Pri}$, $EB_{Pub}$)
BlockchainWallet ← createBlockchainWallet($P_{Pub}$,$P_{Pri}$);
(professorID,$P_{Pri}$) ← safelyStore(professorID, $P_{Pri}$ );
transaction ← sendTransaction( );
```

4.3 Professor Setting and Sharing Questions with Exam Board (EB)

The professor sets the questions and encrypts the questions_file with the symmetric key using AES algorithm to produce a cipher text file C. The professor then shares the symmetric key with EB using Diffie-Hellman key exchange. In order to ensure that the questions come from a valid source, the hash of the questions file is generated using SHA256 and the resultant hash is signed with the private key of the professor using Elliptic Curve Digital Signature Algorithm (ECDSA). The cipher text C and the signature along with a time stamp is sent as a transaction to EB's blockchain address. The transaction is processed through blockchain network. The process is summarised in Algorithm 3.

Algorithm 3: Setting and Sharing Questions with EB

```
($K_{Sym}$) $\leftarrow$ generateSymmetricKey( );
Share the symmetric key $K_{Sym}$ with EB using Diffie-Hellman key exchange.
C $\leftarrow$ Encrypt_AES(questions_file, $K_{Sym}$);
$hash_{Ori}$ $\leftarrow$ hash_SHA256(questions_file);
Signature $\leftarrow$ sign_ECDSA($hash_{Ori}$, $P_{Pri}$)
transaction $\leftarrow$ sendTransaction(C, Signature, TimeStamp, EB's Blockchain Address);
```

4.4 Receiving of Questions by Exam Board (EB)

Algorithm 4 represents the process of receiving questions by the EB. EB receives the encrypted questions file C and the signature as a transaction from the professor. The received C is decrypted with the symmetric key K_{Sym} using AES algorithm to recover the original questions file. EB generates the hash value $hash_c$ of the decrypted file using SHA256. EB then feeds the received signature to the verification algorithm so as to extract $hash_{Ori}$. If both $hash_{Cal}$ and $hash_{Ori}$ matches, it implies that the questions are not tampered. The retrieved questions are then stored in the local database. The professor is then paid and a smart contract is executed that automatically revokes the access right of the professor.

Algorithm 4: Receiving of Questions by NTA

```
questions_file $\leftarrow$ Decrypt_AES(C, $K_{Sym}$);
$hash_{Cal}$ $\leftarrow$ hash_SHA256(questions_file);
Using the professor's $P_{Pub}$, extract $hash_{Ori}$
if $hash_{Cal}$ equals $hash_{Ori}$ then
    return "Signature Valid"
else
    return "Signature Invalid"
Store the questions file in the local database
amount $\leftarrow$ payProfessor(amount, Professor's Blockchain Address);
smartContract_revokeAccess(professorID)
```

4.5 Processing of Questions by Moderators

The moderators will then be assigned with the privilege to read and modify the questions by the EB. The process of moderating, selecting and preparing the final set of question papers is represented in Algorithm 5. The moderators would assess the quality and difficulty of the questions. Once the consensus among different moderators is reached on the final set of questions that can be used for the exam, different sets of question papers (QP) can then be created randomly. Further, the question papers undergo formatting where, if required, they can be translated into native languages and is locked from further access until the date of the exam. The final set of question papers are again encrypted and the hash of the files of stored on the blockchain network. The rights of the moderator from further access to question papers can be revoked by executing a smart contract.

Algorithm 5: Processing of Questions by Moderators

```
questions_file[ ] $\leftarrow$ receiveQuestions( );
Assess the quality and difficulty
Final Questions $\leftarrow$ consensus_Moderators( )
Prepare different sets of QP with appropriate formatting as required
for each QP in the set
    Encrypt and store in the local database along with a timestamp
    $Hash_{QP}$ $\leftarrow$ hash_SHA256(QP);
    Store the $Hash_{QP}$ in the blockchian network
End for
smartContract_revokeAccess(modertorID)
```

4.6 Student taking up the exam

The students can then appear for the entrance in selected centre using their admit cards. On the specified date and time, a smart contract is executed that broadcasts the question paper randomly across the different student nodes along with a key to the student's blockchain address. The student can then unlock the question paper using the key and take up the exam. On completion of the exam by a student, the question number and their corresponding answers are saved as a transaction in the blockchain network. The process is summarised in Algorithm 6.

Algorithm 6: Student taking up the exam

```
Decrypt the QP stored in the local database before the exam
QP_ID, QP, key ← smartContract_randomlySendQP(QP_ID, key, student's Blockchain address );
Unlocked QP ← unlockQP(QP,key)
Take up the exam
if currentTime = = examEndTime || clickFinish = = true
    store the QP_ID, Question Number_Answer[ ][ ], and Timestamp on the blockchain network
end if
```

4.7 Preparing and Sending the Score Card to Students

The process of preparing and sending the score card to students in summarised in Algorithm 7. After the exams, a smart contract can be used to verify the answers and prepare a score card listing the final score, listing the score in each category, the cut-off and validity for each student. The score card also contains the duration of its validity. When the file is uploaded to IPFS, it generates the hash of the file that always starts with Qm… After which the file is available on the IPFS network. The IPFS code of the score card will be sent to the corresponding student's blockchain address. The student then feeds the received signature to the verification algorithm to check if hash value received matches with the calculated hash value. Matching implies that the score card is not tampered. The transactions is processed through blockchain network.

Algorithm 7: Preparing and Sending Score Card to Students

```
Score Card ← smartContract(studentID, QP_ID, Question Number_Answer[ ][ ])
$IPFS_{Hash}$← Uploaded the Score card file to IPFS network to generate the hash code and make it subsequently accessible.
$Signature_{EB}$← sign_ECDSA($IPFS_{Hash}$, $EB_{Pri}$)
transaction ← sendScoreCardtoStudent($IPFS_{Hash}$, $Signature_{EB}$, TimeStamp, Student's Blockchain Address);
verify signature
```

4.8 Universities Verifying Student's Score Card

The university can verify the student's score card to ensure authenticity, reliability and validity. The student can send the $IPFS_{Hash}$ of the score card signed with his/her private key. The university can check the signature to ensure the authenticity and reliability. The process is depicted in Algorithm 8.

Algorithm 8: Universities Verifying Student's Score Card

```
Receive $IPFS_{Hash}$, $Signature_{EB}$, $Signature_{Stud}$
Execute a Smart Contract to validate the signature of the Exam Board and Student and the Score Card Validity period
if Score Card is valid then
    if $Signature_{EB}$ and $Signature_{Stud}$ is valid
        return "Score Card Valid"
    else
        return "Score Card Invalid"
    end if
else
    return "Score Card Invalid"
```

5. Comparison with existing Solutions

A comparative study between the proposed framework and the existing blockchain solutions such as Islama et al., (2019) and Pee et al., (2019) is given in Table 1.

Table 1: Comparison between proposed framework and existing solutions

Features	Islama et al., (2019)	Pee et al., (2019)	Proposed Framework
Secure Login	✓	✓	✓
Random QP Generation	✓	✓	✓
Encryption of QP	✓	✓	✓
Random Selection of QP	✓	✓	✓
Timestamp Lock	✓	✓	✓
Distributed Sharing of QP	✓	✓	✓
Online Exam Support	✗	✓	✓
Support for Universities to Verify the Score Card	✗	✗	✓

6. Conclusion and Future Work

In this paper, a framework for conducting entrance examination online and verifying the score card on top of Blockchain technology is proposed. The proposed framework is highly decentralized, transparent and reliable. As the records in the blockchain cannot be altered or deleted, the proposed framework alleviates the issues faced in the centralized exam systems such as paper leaks, copying, forging of exam results and forging of certificates. Our future plan is to test and evaluate the proposed framework in a real time environment.

References

Arndt, T. (2018). *Empowering University Students with Blockchain-Based Transcripts*. In Proceedings of CELDA 2018. Budapest, Hungary, October 21-23.

Aste, T., Tasca, P., Di Matteo, T. (2017). *Blockchain Technologies: The Foreseeable Impact on Society and Industry*. Computer, 50, 18–28.

Ayed, A.B. (2017). *A Conceptual Secure Blockchain-based Electronic Voting System*. International Journal of Network Security & Its Applications, 9(3).

Azaria, A., Ekblaw, A., Vieira, T., and Lippman, A. (2016). *MedRec: Using Blockchain for Medical Data Access and Permission Management*. 2016 2nd International Conference on Open and Big Data (OBD), 25-30.

Bandara, I., Ioras, F., and Arraiza, M.P. (2018). *The emerging trend of blockchain for validating degree apprenticeship certification in cyber security education*. INTED2018 Conference, 7677–7683.

Bansal, P. Panchal, R., Bassi, S., and Kumar, A. (2020). *Blockchain for Cybersecurity: A Comprehensive Survey*. 2020 IEEE 9th International Conference on Communication Systems and Network Technologies (CSNT), 260-265.

Bitcoin Wiki. (2021). *Genesis Block*. https://en.bitcoin.it/wiki/Genesis_block

Bitshares. (2014). *Your Share in the Decentralized Exchange*. [Online]. Available: https://bitshares.org/

Christidis, K. and Devetsikiotis, M. (2016). *Blockchains and smart contracts for the Internet of Things*. IEEE Access, 4, 2292–2303.

Abhishek Kumar, Pramod Singh Rathore, Vishal Dutt, (2019) "*An IOT Method for Reducing Classification Error In Face Recognition With The Commuted Concept Of Conventional Algorithm*", International Journal of Innovative Technology and Exploring Engineering (IJITEE), ISSN: 2278-3075, 8(11).

Dziembowski, S. Faust, V. Kolmogorov, and K. Pietrzak. (2015). *Proofs of space*. In Advances in Cryptology– CRYPTO 2015, 585-605.

Elisa, N., Yang, L., Chao, F., and Cao, Y. (2018). *A framework of blockchain based secure and privacy-preserving E-government system*. Wireless Networks, 1 - 11.

Gräther, W., Kolvenbach, S., Ruland, R., Schütte, J., Torres, C., and Wendland, F. (2018). *Blockchain for Education: Lifelong Learning Passport*. In Proceedings of 1st ERCIM Blockchain Workshop 2018.

Vishal Dutt, Sriramakrishnan Chandrasekaran, Vicente García-Díaz, (2020). *Quantum Neural Networks For Disease Treatment Identification*. European Journal of Molecular & Clinical Medicine, 7(11), 57-67.[

Islama, A., Kaderb, Md. F., Shin, S. Y. (2019). *BSSSQS: A Blockchain Based Smart and Secured Scheme for Question Sharing in the Smart Education System*. Journal of Information and Communication Convergence Engineering, 17(3), 174-184.

Kassab, M. H., DeFranco, J., Malas, T., Laplante, P., Destefanis, G., and Graciano Neto, V. V. (2019). *Exploring Research in Blockchain for Healthcare and a Roadmap for the Future*. IEEE Transactions on Emerging Topics in Computing, 1-1.

Kuvshinov, K., Nikiforov, I., Mostovoy, J., and Mukhutdinov, D. (2018). *Disciplina: Blockchain for Education*.

Li, L., Liu, J., Cheng, L., Qiu, S., Wang, W., Zhang, X., and Zhang, Z. (2018). *CreditCoin: A Privacy-Preserving Blockchain-Based Incentive Announcement Network for Communications of Smart Vehicles*. IEEE Transactions on Intelligent Transportation Systems, 19(7), 2204-2220.

Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. https://bitcoin.org/bitcoin.pdf

S. R. Swarna, S. Boyapati, V. Dutt and K. Bajaj, "*Deep Learning in Dynamic Modeling of Medical Imaging: A Review Study*," 2020 3rd International Conference on Intelligent Sustainable Systems (ICISS), Thoothukudi, India, 2020, pp. 745-749, doi: 10.1109/ICISS49785.2020.9315990. MIT Media Lab. (2017). *Certificates, Reputation, and the Blockchain*. Retrieved October 10, 2017 from http://certificates.media.mit.edu/

Nguyen, G. T. and Kim, K. (2018). *A Survey about Consensus Algorithms Used in Blockchain*. J Inf Process Syst, 14(1), 101-128.

Park, S., Pietrzak, K., Kwon, A., Alwen, J., Fuchsbauer, G., and Gazi, P. (2017). *Spacecoin: a cryptocurrency based on proofs of space*. [Online]. Available: https://eprint.iacr.org/2015/528

Paul J. Taylor, Tooska Dargahi, Ali Dehghantanha, Reza M. Parizi, Kim-Kwang Raymond Choo, (2020), “A systematic literature review of blockchain cyber security”, Digital Communications and Networks, 6(2), 147 - 156.

S. Boyapati, S. R. Swarna, V. Dutt and N. Vyas, "*Big Data Approach for Medical Data Classification: A Review Study*," 2020 3rd International Conference on Intelligent Sustainable Systems (ICISS), Thoothukudi, India, 2020, pp. 762-766, doi: 10.1109/ICISS49785.2020.9315870.

P4Titan. (2014). *Slimcoin: a peer-to-peer crypto-currency with proof-of-burn*. [Online]. Available: http://www.doc.ic.ac.uk/~ids/realdotdot/crypto_papers_etc_worth_reading/proof_of_burn/slimcoin_white paper.pdf.

Rouhani, S., Butterworth, L., Simmons, A. D., Humphery, D. G., and Deters, R. (2018). MediChainTM: A Secure Decentralized Medical Data Asset Management System. 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), 1533-1538.

A.Dubey,A.Kumar,R.Agrawal. “*An efficient ACO-PSO based framework for data classification and preprocessing in big data*" published in Evolutionary Intelligence Springer Electronic ISSN 1864-5917,Print ISSN 1864-5909

Salha, R.A., El-Hallaq, M.A. and Alastal, A.I. (2019). *Blockchain in Smart Cities: Exploring Possibilities in Terms of Opportunities and Challenges*. Journal of Data Analysis and Information Processing, 7(3), 118 - 139.

Sharples, M., and Domingue, J. (2016). *The blockchain and kudos: a distributed system for educational record, reputation and reward*. In: Verbert, K., Sharples, M., Klobučar, T. (eds.) EC-TEL 2016. LNCS, vol. 9891, pp. 490–496. Springer, Cham.

S.Chandrasekaran and A.Kumar, “*Implementing Medical Data Processing with Ann with Hybrid Approach of Implementation Journal of Advanced Research in Dynamical and Control Systems*”, JARDCS issue 10, vol.10, page 45-52, ISSN-1943-023X. 2018/09/15.

Turkanović, M., Hölbl, M., Košič, K., Heričko, M., Kamišalić, A. (2018). *EduCTX: a blockchainbased higher education credit platform*. IEEE Access 6, 5112–5127.

Xia, Q. I., Sifah, E. B., Asamoah, K. O., Gao, J., Du, X., & Guizani, M. (2017). *MeDShare: Trust-less Medical Data Sharing among Cloud Service Providers via Blockchain*. IEEE Access, 5, 14757-14767.

Xia, Q., Sifah, E., Smahi, A., Amofa, S., and Zhang, X. (2017). *BBDS: Blockchain-Based Data Sharing for Electronic Medical Records in Cloud Environments*. Information (Switzerland), 8(2), 44.

Pramod Singh Rathore, Abhishek Kumar, Vicente García-DíazSpringer, “*A Holistic Methodology for Improved RFID Network Lifetime by Advanced Cluster Head Selection using Dragonfly Algorithm*”, IJIMAI, - ISSN 1989-1660.

Yuan, Y. and Wang, F. (2016). *Towards blockchain-based intelligent transportation systems*. 2016 IEEE 19th International Conference on Intelligent Transportation Systems (ITSC), 2663-2668

Zheng, Z., Xie, S., Dai, H., Chen, X., and Wang, H. (2017). *An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends*. In Proceedings of the 2017 IEEE International Congress on Big Data (BigData Congress), Boston, MA, USA, 11– 14 December 2017, 557–564.