IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 8, Issue 8, August 2020

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.488

9940 572 462 | 6381 907 438 | ijircce@gmail.com | www.ijircce.com

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | Impact Factor: 7.488 |

|| Volume 8, Issue 8, August 2020 ||

BTES: Blockchain Technology In Education System " A Smart Solution for Facing a Threat of Question Paper Leaking"

Anita Dhami[1], Prof. Dr. D.R. Ingle [2]

M.E. Student, Department of Computer Engineering, Bharati vidyapeeth college of Engineering , Navi .Mumbai, India[1]

HOD Of Computer Department, Bharati Vidyapeeth College Of Engineering, Navi Mumbai, India[2]

ABSTRACT: To address the challenges of current education system, applied approach is called Blockchain Technology In Education System(BTES). Blockchain is a disruptive technology, after a few years of implementation as the basis of digital currency, is showing itself to be an open resource with possibilities in different fields, also in education system .The key to the interest in this technology lies in its ability to move from a system of centralized data logging to a distributed system that ensures no alteration of the information and the maintenance of privacy. The purposed system present the improved examination system for addressing the challenges of paper leaks problems and also focusing the fake college diploma /Degree and other qualifications , is a huge problem in this age of professional-grade copying and printing services .To verify the authenticity of academic certificates and preventing the paper leak problem , proposed model employing a block chain technology, because of its greater security and transparency.

KEYWORDS: Blockchain, decentralized ledger, cryptographically, randomization algorithm.

I. INTRODUCTION

Blockchain is a distributed and decentralized technology (P2P) [8]which can be used to record transactions, agreements, contracts and events. In essence, block sites of records or public accounting are a distributed database of all digital transactions or events that have been completed and shared between the participating parties. Unlike other general accounting approaches, blockchain guarantees archiving of approved transactions without proof of intermediary. All transactions in the public ledger are verified with the consent of the majority of participants in the system. And, when submitted, the information cannot be deleted. Blockchain include a true and verifiable record of all transactions carried out.

Blockchain was originally developed to support cryptocurrency, Bitcoin (Nakamoto, 2008)[18], a point-to-point decentralized digital currency, which is the most common example of blockage technology. With Bitcoin's success, the original blockchain technology worked perfectly and has found a wide range of applications in both financial and non-financial worlds. A blockchain is a growing list of records, called blocks, which are linked using cryptography. Each block contains a cryptographic hash of the previous block a timestamp, and transaction data (generally represented as a Merkle tree).

The exam is one of the important parts of the education system because it not only assesses students' understanding, but also forces them to study. However, there is a threat, called Question Paper Leaking (QPL), which can cause equity problems in exams. Today, the QPL is a serious problem worldwide, from the university entrance exam to the public exam, and the situation is worse in developing countries [5, 6,]. QPL can lead to serious results, such as (1) quality of compromised education and (2) erosion of ethical standards. ACT Inc, who is the creator of the most popular college entrance exam in the United States, canceled some college entrance exams after losing the exam material [7]. In the United Kingdom, Brighton Hove and Sussex Sixth Form College have canceled the level A physics exam after noticing the escape of questions on social media [3]. In China, a teacher was accused of leaking a postgraduate exam math test document [9]. Though the above-mentioned cases [3,5,6,7,9] only covers the QPL incidents happened in 2017, some countries face this problem almost in every year. Hence, it can be said that QPL happens not only within the developing and underdeveloped countries, but also in developed countries. In QPL incidents, not only the students, but also the teachers and authorities are involved. Therefore, it is required to develop a smart examination system which can create and share examination papers securely without the fear of QPL.

To overcome to this problem, we used the concept of block chain technology in BIES/BTES. For constructing and distribution of question paper. Blockchain can be one of the promising techniques to provide security against the above-

mentioned threats. The BIES technique is proposed to encrypt the question papers (QSP). In first phase, the QSPs are encrypted using the timestamp and in the second phase, the previous encrypted QSPs are encrypted again using hashish and hash of the previous QSPs. These encrypted QSPs are stored in the blockchain network (university's Server).

II. RELATED WORK

The research work is done in blockchain based related application in [1,2,5,9,13,20,16,18,20].
The OmniPHR[1] which focuses on the distribution and interoperability of PHR (Personal Health Records) data, in which patients, by definition, can manage their health records, generally have no control over their stored data in the database of health workers[1]. In MeDShare (Medical Data Sharing) [2], a system that addresses the problem of exchanging medical data between medical big data custodians in an untrusted environment. The system is based on the blockchain and provides provenance, auditing and control of medical data shared in cloud repositories between big data entities. In paper[5] author proposed the digital platform and governance regime interplay as an important factor for disruptive derivatives to be developed. The governance model in public administration is centralized, and that introducing a new digital platform like Bitcoin could foster new disruptive derivative services in public sector, but at the same time could challenge the centralized governance model. The blockchain technology adopts basic cryptographic algorithms [9]and schemes for consensus and transaction authentication, such as hash functions, digital signatures and so on. But these technologies can not satisfy the security requirements in the complex business environment and the attacks that may appear in the future[9].

III. PROPOSED SYSTEM

Existing education systems are facing a threat of question paper leaking (QPL) in the exam which endangers the quality of education. In this paper, we use the concept of Blockchain Tecgnologyin education system (termed as BTES) The proposed scheme can increase application security and provide a smooth exchange between the examcenters

- A two-phase encryption technique (which uses different parameters as a key) is proposed to ensure security question.
- A randomization algorithm is proposed to select a questionnaire and share question paper before the exam.

We develop a QS scheme which uses blockchain concept in order to make it secure and smart. The proposed BTES is a new way of generating & sharing questions. There are following major entities involved in this system , as shown in Fig. 1. Each of the entities is described in the following sections.

Module 1:Blockchain Node: This module is very important for functioning of this network. To configure particular node in network, its security parameters need to set and public key and other parameters will be broadcasted to other nodes.

Module 2: University Module: University is organisation which will be responsible for mapping educations blockchain. University will add colleges in blockchain network and also responsible for making blockchain from parameter for colleges

Module 3: College Module: Ones University added college in blockchain network College Model provide functionality for configuration security key and digital signature. Client will add private key for encryption and publish his public key in blockchain network.

Module 4:Exam Module: University will declare exam for different courses and that will be added to blockchain network as block .This module allow University to give permission to some colleges to set question paper and final functionality of this module is to allow colleges to access question paper securely from blockchain network on the day of exam to ensure that there will not be any escape of question paper

Module 5:Question Paper Module: Once university grant permission to respective colleges , will be add question for question paper these questions will be added as a block in blockchain network. All block have data in encrypted format and auto registration is assured by Digital Signature

Module 6: Blockchain Module:This module will be responsible for adding block to blockchain network. This module will form chain of block security, authentically. This module also provide functionality to access blocked from blockchain Network and ensure data is not tempered and also validated authenticity of block.

Module 7: Document and certificate Module: Once student take admission and complete Course from respective education institute will add all general document and certificate in blockchain network so , student will not have submit same document again in same college or different colleges .All these document will be share very securly through blockchain network .

This will prevent illegal certification generation and save paper for tree and save nature.

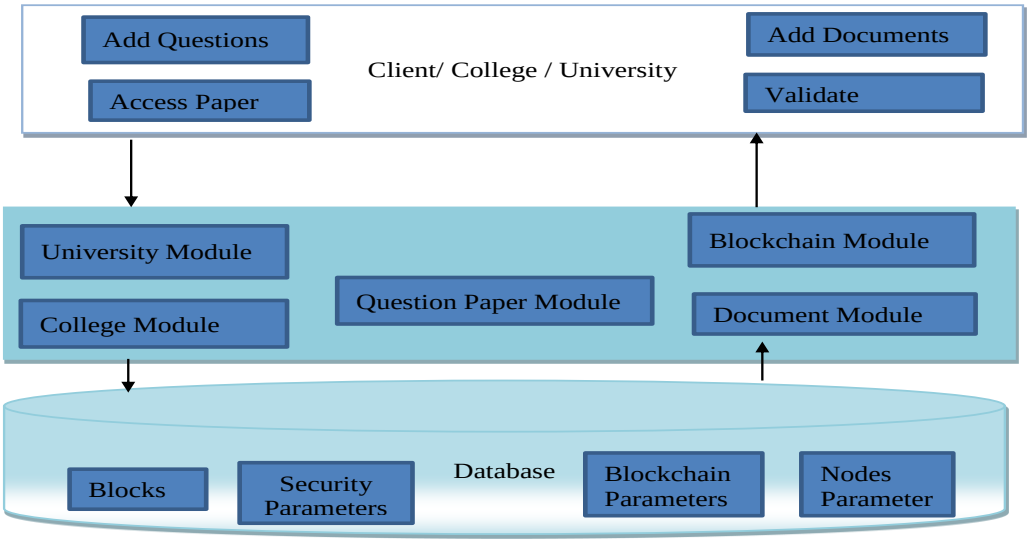


Fig 1. System model of the proposed (BTES)

ADescription of the Algorithm

Random question and question paper selection - This feature supports the selection of a QSP randomly before the exam. The benefits of the random selection of QSP is that no one can guess the selected QSP.Thescheme that no one can decipher the Question paper. Hence zero % chance of paper disclosed.

A blockchain is a growing list of records, called blocks, which are linked using cryptography. Each block contains a cryptographic hash of the previous block a timestamp, and transaction data (generally represented as a Merkle tree).

By design, a blockchain is resistant to modification of the data. It is "an open, distributed ledger that can record transactions between two parties efficiently and in a verifiable and everlasting way.we propose the following Blockchain mechanisms.

Thus, node A will change the messages into the following form:

$$M_A = E(r \oplus k^*, k^*)|| M || r||HK * ID^A$$

After G decrypts K* using the pre-distributed key k*and r, and verifies K* using H(K*), it can ensure that MA comes from a legal college node because only legal college nodes have the Pre distributed key k*. G should use digital signature algorithm to sign messages using its private key before broadcasting these messages. Thus, blockchain nodes will know which college node have broadcasts.

$$Mg = M||r||H(k^*)|| ID_A||B_A$$

and then the broadcasted messages have the following form:

$$E(K, Mp)||Mg||Sig(Kpg, H(E(K, Mp)||Mg))$$

Here, Sig(.) denotes the signature algorithm and Kpg the private key of college node. After each blockchain node receives the message, it can verify the message by using the public key of G. According to the consensus mechanism, if blockchain nodes believe G is a legal device and the signature is valid, they will put on the A-chain.

$$E(K, Mp)||Mg$$

If G is illegal node or the message's signature send by G is invalid, blockchain nodes will put

$$Sig(Kpg, H(E(K, Mp)||Mg||Mw|| MSig(Sig(Kpg, H(E(K *, Mp)||Mg||Mw$$

on the B-chain to record the accident. Here, Msig(.) denotes a broadcasting multidigit signature scheme executed by blockchain nodes. Mw records the broadcasting time of physiological messages and the reason of rejection. For the sake of saving storage, B-chain need not to store (E(K*,Mp)||Mg). When G asks question about the rejection, it can inquire B-chain by clues:

Sig (Kpg, H(E(K*,Mp)||Mg)) and the messages' broadcasting time.

So all data generate by college nodes will be encrypted by nodes private key and hash of message will be appended to block and each block is sign by digital signature to verify authenticity and authentication.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | Impact Factor: 7.488 |

|| Volume 8, Issue 8, August 2020 ||

IV. PSEUDO CODE

```
Algorithm add_Node (node)
{
        checkAlreadyExist(node)
{
Break;
} else {
        Check security Parameters
        Check Network Configuration
        Configure Node in Peer to Peer Network
        Configure Security Parameter
        Update Blockchain Network
}
}
Algorithm add_block (data)
{
        Var edata=encrypt(data);
        Var hash= SHA (data);
        Var Block=null;
        Get Previous blockid;
        Prepare block with all details and assign to block;
```

$$\text{Block} = M_A = E(r \oplus k^*, k^*) || M || r || HK * ID^A$$

```
                Var digiSign=Sig(Kpg, H(E(K, Mp)||Mg));
Broadcast message in blockchain network;
Upon nodes receive message verify digital Signature put encrypted block on blockchain network
```

$$E(K, Mp)||Mg$$

```
        Index the inserted block for future search;

}
```

```
Algorithm accessblock (ref)
{
        Access indexed block;
        Verify digital Signature;
        If(digital Signature invalid ){
                Record it with as accident
Sig(Kpg, H(E(K, Mp)||Mg||Mw|| MSig(Sig(Kpg, H(E(K *, Mp)||Mg||Mw
        }
        Verify hash value;
        Decrypt the data;
}

Algorithm examblockchain(exam)
{
        Announce the exam;
        Add announced exam as block in blockchain network
  //add_block(exam);
        University select professors from different colleges to set the exam paper;
        Professors set the question will be added as block in blockchain network
                //add_block(questions);
        On date of exam university release the paper just before exam;
        Random blocks from exam questions will be selected
                // accessblock (examid)

        Print decrypted paper
}
```

V. SIMULATION RESULTS

Existing System Paper's Selection Process

- Papers are made by 4–5 resource professors .
- No paper is handwritten, all submitted in print
- Papers go to moderators who check the difficulty level and finalize one
- Send for translation and then printed
- Papers sent to storage
- Sent to the regional office (RO). RO sends it to custodian bank
- Picked up from bank on exam day
- Sent to exam centre, where the seal is broken. Papers distributed to the invigilators
- Authorities watching over all of the above activities

The proposed system will use blockchain technology to make current education system more reliable, Simple, authenticate, and secure.

BTES Based Paper's Selection Process

- The proposed system will establish blockchain network of education institutes.
- University allocate nodes for paper selection.
- The professor would upload their paper on blockchain network .
- Paper will be encrypted by hash function.
- It can lock down for access until due date.

- On the exam date paper will be accessible and decrypted for exam centres.

SCREENSHOT OF BIES/BTES

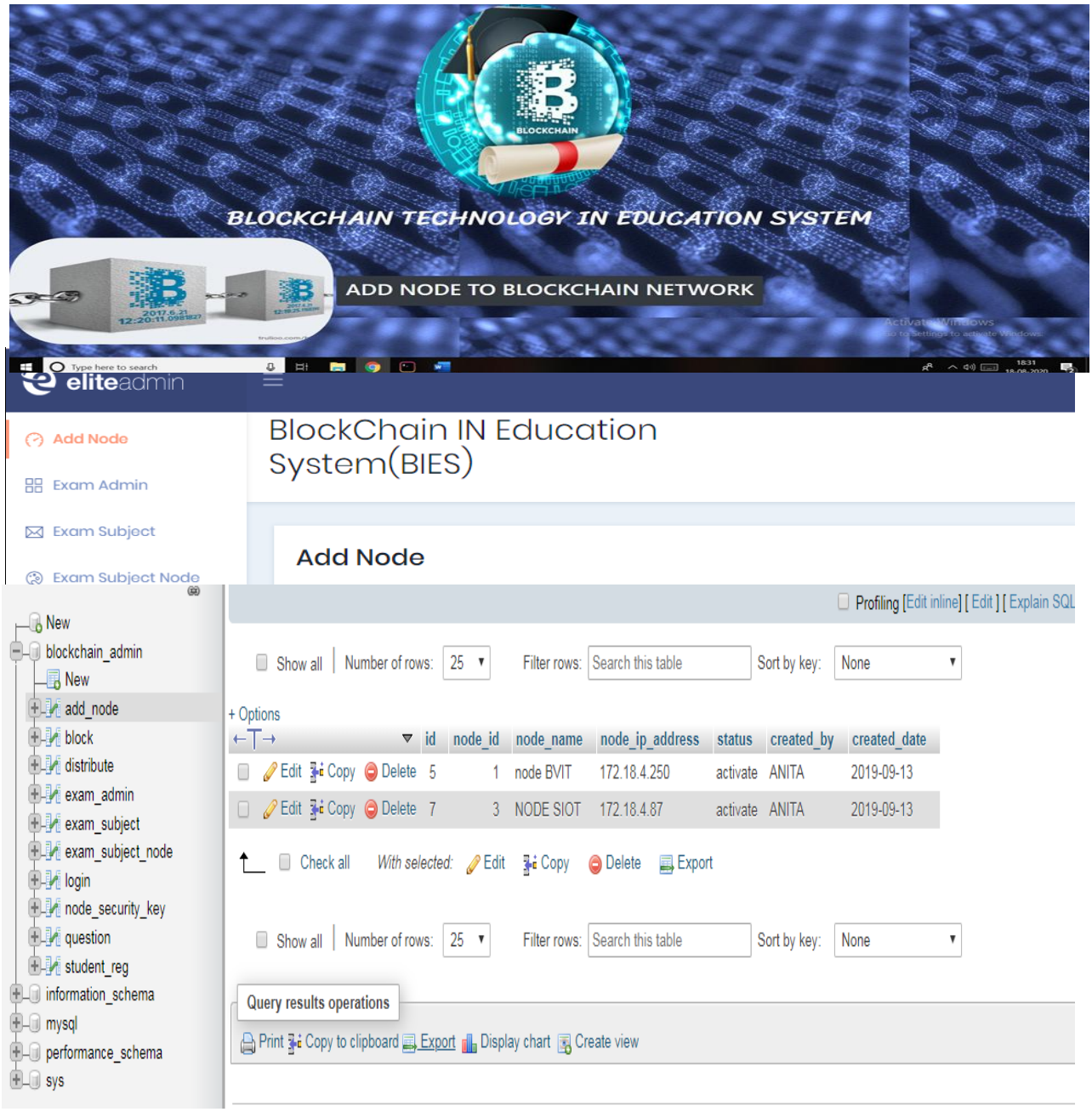


Fig.1.1 Adding Node into Blockchain Network

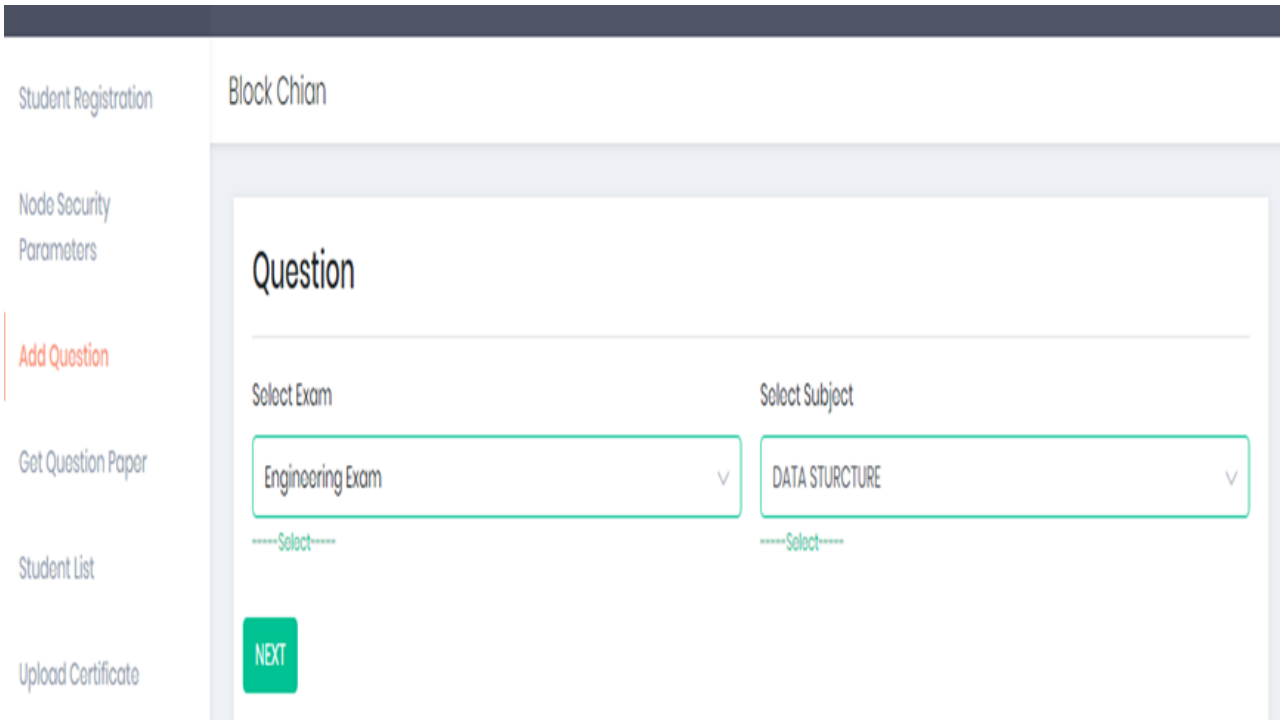
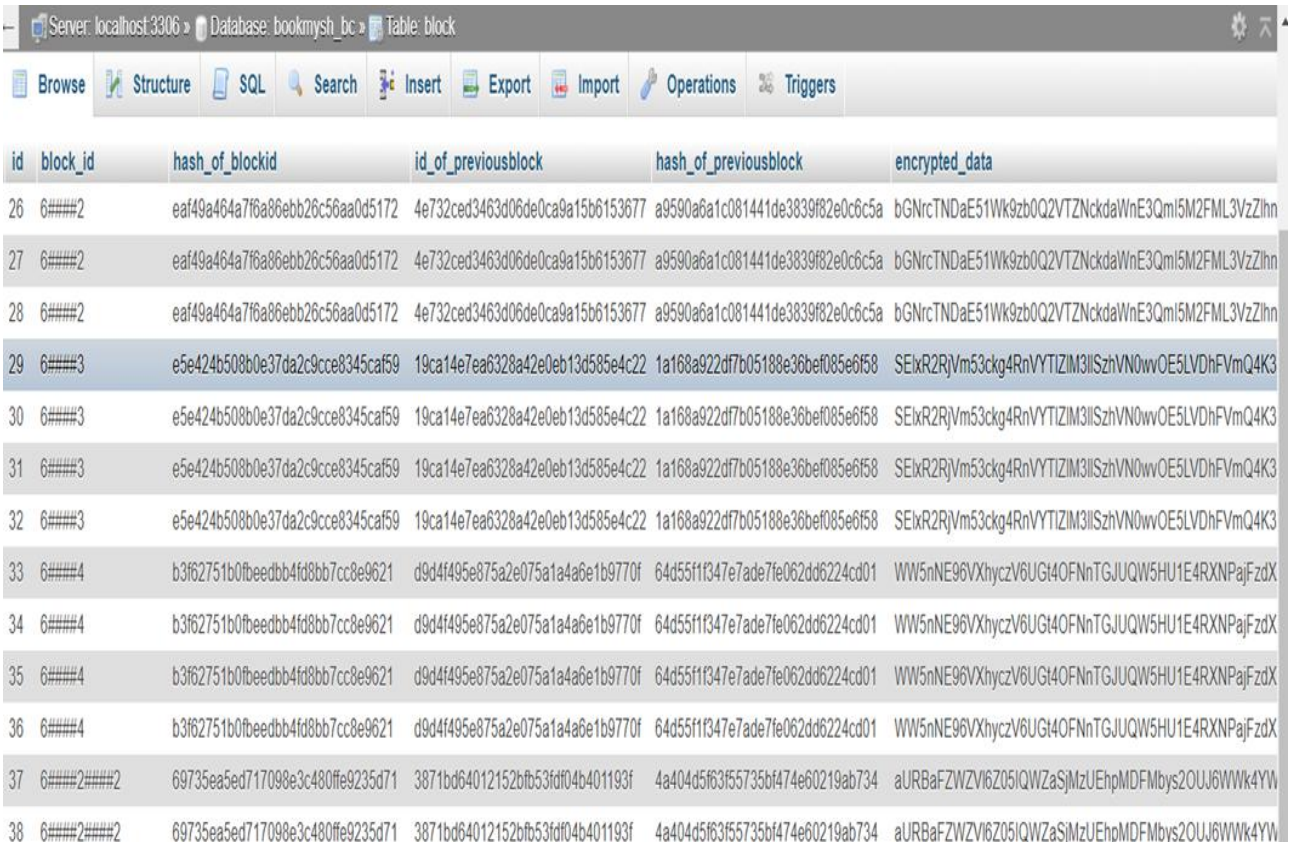


Fig.1.2 Exam Adding module



id	block_id	hash_of_blockid	id_of_previousblock	hash_of_previousblock	encrypted_data
26	6####2	eaf49a464a7f6a86ebb26c56aa0d5172	4e732ced3463d06de0ca9a15b6153677	a9590a6a1c081441de3839f82e0c6c5a	bGNrcTNDaE51Wk9zb0Q2VTZNckdaWnE3Qml5M2FML3VzZlhn
27	6####2	eaf49a464a7f6a86ebb26c56aa0d5172	4e732ced3463d06de0ca9a15b6153677	a9590a6a1c081441de3839f82e0c6c5a	bGNrcTNDaE51Wk9zb0Q2VTZNckdaWnE3Qml5M2FML3VzZlhn
28	6####2	eaf49a464a7f6a86ebb26c56aa0d5172	4e732ced3463d06de0ca9a15b6153677	a9590a6a1c081441de3839f82e0c6c5a	bGNrcTNDaE51Wk9zb0Q2VTZNckdaWnE3Qml5M2FML3VzZlhn
29	6####3	e5e424b508b0e37da2c9cce8345caf59	19ca14e7ea6328a42e0eb13d585e4c22	1a168a922df7b05188e36bef085e6f58	SElxR2RjVm53ckg4RnVYTlZlM3llSzhVN0wvOE5LVDhFVmQ4K3
30	6####3	e5e424b508b0e37da2c9cce8345caf59	19ca14e7ea6328a42e0eb13d585e4c22	1a168a922df7b05188e36bef085e6f58	SElxR2RjVm53ckg4RnVYTlZlM3llSzhVN0wvOE5LVDhFVmQ4K3
31	6####3	e5e424b508b0e37da2c9cce8345caf59	19ca14e7ea6328a42e0eb13d585e4c22	1a168a922df7b05188e36bef085e6f58	SElxR2RjVm53ckg4RnVYTlZlM3llSzhVN0wvOE5LVDhFVmQ4K3
32	6####3	e5e424b508b0e37da2c9cce8345caf59	19ca14e7ea6328a42e0eb13d585e4c22	1a168a922df7b05188e36bef085e6f58	SElxR2RjVm53ckg4RnVYTlZlM3llSzhVN0wvOE5LVDhFVmQ4K3
33	6####4	b3f62751b0fbeedbb4fd8bb7cc8e9621	d9d4f495e875a2e075a1a4a6e1b9770f	64d55f1f347e7ade7fe062dd6224cd01	WW5nNE96VXhyczV6UGt4OFNnTGJUQW5HU1E4RXNPajFzdX
34	6####4	b3f62751b0fbeedbb4fd8bb7cc8e9621	d9d4f495e875a2e075a1a4a6e1b9770f	64d55f1f347e7ade7fe062dd6224cd01	WW5nNE96VXhyczV6UGt4OFNnTGJUQW5HU1E4RXNPajFzdX
35	6####4	b3f62751b0fbeedbb4fd8bb7cc8e9621	d9d4f495e875a2e075a1a4a6e1b9770f	64d55f1f347e7ade7fe062dd6224cd01	WW5nNE96VXhyczV6UGt4OFNnTGJUQW5HU1E4RXNPajFzdX
36	6####4	b3f62751b0fbeedbb4fd8bb7cc8e9621	d9d4f495e875a2e075a1a4a6e1b9770f	64d55f1f347e7ade7fe062dd6224cd01	WW5nNE96VXhyczV6UGt4OFNnTGJUQW5HU1E4RXNPajFzdX
37	6####2####2	69735ea5ed717098e3c480ffe9235d71	3871bd64012152bfb53fdf04b401193f	4a404d5f63f55735bf474e60219ab734	aURBaFZWZVl6Z05lQWZaSjMzUEhpMDFMbys2OUJ6WWk4YW
38	6####2####2	69735ea5ed717098e3c480ffe9235d71	3871bd64012152bfb53fdf04b401193f	4a404d5f63f55735bf474e60219ab734	aURBaFZWZVl6Z05lQWZaSjMzUEhpMDFMbys2OUJ6WWk4YW

Fig.1.3 Hash and Encrypted Data in Database

Fig.1.4 Paper distribute successfully

VI. CONCLUSION AND FUTURE WORK

This project proposes the new scheme for intellectual education, using the blockchain concept, the cryptography technique is used for the creation and exchanges of question papers (QSP). In the first phase, the QSPs are encrypted using the encrypted session ID and in the second phase, the previous encrypted QSPs are re-encrypted using the hashish and hash of the previous QSPs. These encrypted QSPs are stored in the blockchain together with a university device. An algorithm is also proposed to select a QSP for the exam, such as selecting a random question from different application documents. The scheme according to which nobody can decipher the document of the application. Furthermore, the proposed system can also be used to store and share confidential documents with little or no modification, here we can only show some module and in detail which could be subject to future work

Therefore, it can be said that BTES can be a promising approach for providing proper security to mitigate QPL problem in the future smart education system. Furthermore, the proposed system can also be used to share sensitive documents with little or no modification, which can be subjected to future works

REFERENCES

1. Alex Roehrs, Cristiano André da Costa , Rodrigo da Rosa Righi Journal of Biomedical Informatics 71 (2017) 70–81. “OmniPHR: A distributed architecture model to integrate personal healthrecords”.
2. Qi Xia, Emmanuel Boateng Sifah, Kwame Omono Asamoah, Jianbin Gao, Xiaojiang Du and Mohsen Guizani IEEE DOI: 10.1109/ACCESS.2017.2730843July 2017 “Trust-less Medical Data Sharing Among Cloud Service Providers Via Blockchain”.
3. R. A. F. Mailonline, Hundreds of students are sent home after A-level physics exam is stolen and shared on social media (May 2017). URL http://www.dailymail.co.uk/news/article-4534118/ Hundreds-students-sent-home-test-paper-leaked
4. S. P. Heyneman, Uses of examinations in developing countries: Selection, research, and education sector management, International Journal of Educational Development 7 (4) (1987) 251 – 263. doi:https: //doi.org/10.1016/0738-0593(87)90023-X.
5. R. Olatoye, Checking the menace of examination malpractice: A call for more teaching and learning in schools, Institute of Education, Olabisi Onabanjo University, Ago-Iwoye, Nigeria (2008).
6. J. McCrank, ACT cancels some college entrance exams after test leak (Sep 2017). URL https://www.reuters.com/article/us-usa-collegecheating/act-cancels-some-college-entrance-examsafter-test-leak-idUSKCN1BI29P
7. Yunhua He 1, (Member, Ieee), Hong Li2, (Member, Ieee), XiuzhenCheng3, (Fellow, Ieee), Yan Liu4, (Member, Ieee), Chao Yang5, (Member, Ieee), And LiminSun2, (Member, Ieee) China April 2, 2018, “A Blockchain Based Truthful Incentive Mechanism For Distributed P2p Applications”.
8. Papers might have been leaked, police tell IoM. URL http://kathmandupost.ekantipur.com/news/2017-11-06/ papers-might-have-been-leaked-police-tell-iom.html”.
9. Wei Yin ,Qiaoyan Wen, Wenmin Li, Hua Zhang, (Member, Ieee), And ZhengpingJin 2018.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | Impact Factor: 7.488 |

|| Volume 8, Issue 8, August 2020 ||

10. html [31] J. Guo, Chinese postgraduate entrance exam leaked? (Dec 2017). URL http://supchina.com/2017/12/27/chinesepostgraduate-entrance-exam-leaked/
11. Oliver, Miquel; Moreno, Joan; Prieto, Gerson; Benítez, David 4thAugust 2018 "Using Blockchain As A Tool For Tracking And Verification Of Official Degrees: Business Model".
12. ShangpingWang1, Yinglong Zhang 1, And YalingZhang , June 24 2018 "A Blockchain-Based Framework For Data Sharing With Fine-Grained Access Control In Decentralized Storage Systems".
13. Exam papers leaked at ukzn (Nov 2017). URL https://www.news24.com/SouthAfrica/News/exampapers-leaked-at-ukzn-20171113
14. Yong Yuan1 And Fei-Yue Wang "Towards Blockchain-Based Intelligent Transportation Systems".
15. A.-M. Al-Youm, French language exam papers leaked on facebook (Jun 2017). URL http://www.egyptindependent.com/french-examsleaked/
16. Vietnam teacher leaks test questions to neighbor as 'return of favor' (May 2017). URL https://tuoitrenews.vn/education/41079/vietnamteacher-leaks-test-questions-to-neighbor-as-returnof-favor
17. Sujit Biswas, Kashif Shaif, Member, IEEE, Fan Li, Member, IEEE, Boubakr Nour, and Yu Wang, Fellow, IEEE march 2018 "A Scalable Blockchain Framework for SecureTransactions in IoT".
18. MuhamedTurkanovi. , Marko Hölbl , Kristjan Ko.I,MarjanHeri.Ko, And Aida Kami.Ali January 5, 2018,."EduCTX: A Blockchain-Based Higher Education Credit Platform ".
19. Racket involved in MDCAT paper leak. URL https://www.thenews.com.pk/print/234932-Racketinvolved-in-MDCAT-paper-leak
20. S. A. S. Correspondent bdnews24.com, Dhaka board holds SSC exam with leaked question paper despite being informed. URL https://bdnews24.com/bangladesh/2017/02/21/dhakaboard-holds-ssc-exam-with-leaked-question-paperdespite-being-informed.

INNO SPACE

SJIF Scientific Journal Impact Factor

Impact Factor:
7.488

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details