INTERNATIONAL JOURNAL OF COMPUTER ENGINEERING AND APPLICATIONS
VOLUME XII, ISSUE VII, July 2018, WWW.IJCEA.COM, ISSN 2321-3469

MAINTAINING AUTHENTICITY OF DIGITAL CERTIFICATE USING BLOCKCHAIN

Sandeep U Kadam[1] , Sunil G. Dambhare[2], Chaitali R Shewale[3], Rupesh J Patil[4]
Associate Professor, Bhivarabai Sawant College of Engineering and Research, Pune, India[1]
Professor, Dr. D. Y. Patil Institute of Engineering Management and Research, Pune, India[2]
Assistant Professor, Keystone College of Engineering, Pune, India[3]
Principal Navsahyadri Grooup of Institutes Faculty of Engineering, Pune , India

ABSTRACT:
According to several researches huge number of graduates are passing out everyyear, the certificate issuing authorities are seems to be compromised for the security credentials of student data. Due to the lack of effective antiforge mechanism, graduation certificates which are copied often get noticed. We can conquer this problem by using digital certificate, though security issues still exist. Blockchain is one of the most recent technologies that can be adopted for the data security. It helps to overcome the problem ofcertificate forgery because of its unmodifiable property. Digital certificate is issued using following procedure. First from student portal and college portal encrypt the entered marks. Then pass this encrypted string to the blockchain. Company portal accepts the marks string from both the portal and passes it to the verification portal. Verification portal decides whether marks are authenticated or not. It will provide the demand unit to verify the genuineness of the paper certificate through mobile phone scanning or website inquiries. Because of the unmodifiable properties of the blockchain, the system not only enhances the authenticity of various paper-based certificates, but also electronicallyreduces the loss risks of various types of certificates.

Keywords— Blockchain, digital certificate, encryption.

[1] Introduction

Advances in data innovation, the wide accessibility of the Internet, and regular useof cell phones have changed the way of life of individuals. Virtual cash, computerized coinsinitially intended for utilize on the web, has started to be widely embraced, overall. Becauseof the comfort of the Internet, different virtual monetary standards are flourishing, includingthe most well-known—Bitcoin, Ether, and Ripple—the estimation of which has flooded asof late. Individuals are starting to focus on blockchain, the spine innovation of these progressive monetary standards.

Blockchain highlights a decentralized and morally sound database that has high potential for a different scope of employments. Blockchain is a circulated database that is broadly utilized for recording particular exchanges. When an agreement is come to among various hubs, the exchange is added to a square that as of nowholds records of a few exchanges. Each square contains the hash estimation of its last partner for association. All the squares are associated and together they structure a blockchain. Satoshi Nakamoto proposed the idea of blockchain in 2008. Blockchain is an online record that gives decentralized and straightforward information sharing. With conveyed accounts, all exchange information (put away in hubs) are packed and added to various squares. Information of different sorts were appropriated in unmistakable squares, empowering checks to be utilized delegates. All the hubs at that point structure a blockchainwith timestamps. The information put away in each square can be confirmed at the same time and become inalterable once entered. The entire procedure is available to the general population, straightforward, and secure. Graduation endorsements and transcripts contain data secret to the people and ought not be effectively open to other people. Thus, there is asignificant requirement for a system that can ensure that the data in such a record is unique,which implies that report has started from an approved source and isn't phony. Furthermore,the data in the archive ought to be private with the goal that approved people must see it. Blockchain innovation is utilized to decrease the occurrence of testament falsifications and

guarantee that the security, legitimacy and secrecy of graduation authentications would be improved. As instruction turns out to be increasingly expanded, decentralized and democratized, we despite everything need to look after notoriety, trust in affirmation, and evidence of learning. These days everybody needs to show his/her Document and Certificate to some other individual for some reason/work. In the wake of seeing, the recordthird individual cannot approve the innovation of the declaration

1. Problem Statement

Graduation certificates and transcripts contain information confidential to theindividuals and should not be easily accessible to others. Hence, there is a high need for a mechanism that can guarantee that the information in such a document is original, which means that document has originated from an authorized source and is not fake. Block chaintechnology is used to reduce the incidence of certificate forgeries and ensure that the security, validity and confidentiality of graduation certificates would be improved.

2. Literature Survey

As indicated by the Taiwan Ministry of Education insights, around one million alumni every year, some of them will go to nations, secondary schools or tertiary foundations to proceed to join in, and some will be prepared to enter the work environment business. Overthe span of study, the understudies' a wide range of astounding execution authentications, score transcripts, recognitions, and so on., will turn into a significant reference for conceding new schools or new works. As schools make different honors or recognitions, just the names of the schools and the understudies are input. Because of the absence of powerful enemy of fashion component, occasions that cause the graduation authentication to be produced regularly get took note. So as to take care of the issue of forging endorsements, the advanced declaration framework dependent on blockchain innovation was proposed in [1]. By the unmodifiable property of blockchain, the computerizeddeclaration with hostile to fake and evidence could be made. The method of giving the computerized authentication right now as follows. To begin with, produce the electronic document of a paper endorsement going with other related information into the database, in the mean time compute the electronic record for its hash esteem. At long last, store the hash an incentive into the square in the chain framework. The framework will make a related QR- code and request string code to attach to the paper declaration. It will give the interest unit to confirm the genuineness of the paper testament through cell phone filteringor site requests. Through the unmodifiable properties of the blockchain, the framework notjust improves the validity of

different paper- based endorsements, yet in addition electronically diminishes the misfortune dangers of different sorts of testaments. Asindicated by different explores around one million alumni spending out every year, the authentication giving specialists are is by all accounts traded off for the security qualifications of understudy information. Because of the absence of successful antiforge system, occasions that cause the graduation authentication to be manufactured frequently get took note. So as to take care of this issue computerized testament frameworks are presented despite the fact that security issues are still exist. Blockchain is one of the latest innovation that can be embraced for the information security. The unmodifiable property of the square chain assists with conquering the issue of declaration falsification. Different instances of the advanced testament framework is referenced in paper [2]. Over the span of training the understudies accomplish numerous endorsements. Understudy produce these testaments while going after positions at open or private segments, where every one of these declarations are should have been checked physically. There can be episodes whereunderstudies may deliver the phony testament and it is hard to recognize them. This issue

of phony scholarly endorsements has been a longstanding issue in the scholastic network. Since it is conceivable to make such testaments requiring little to no effort and the procedureto check them is unpredictable, as they are physically should have been confirmed. This issue can be illuminated by putting away the advanced declarations on the Blockchain. The Blockchain innovation gives permanence and freely irrefutable exchanges, these propertiesof Blockchain can be utilized to produce the computerized declaration which are hostile tofake and simple to check [3]. In the conventional instructive comprehension, people followthe way of getting graduate or post-graduate training in the event that they wish, in the wakeof proceeding with their instruction from kindergarten to secondary school. Today, by escaping this generalization, each educated individual can pick distinctive learning situations. Presently, learning any subject is up to the tip of the fingers of a person withoutrelying upon a school working with four dividers or on certain time period. In [4], it is planned to confirm advanced endorsements given to the members at the Turkish phase of the International Informatics and Computational Thinking occasion by utilizing Ethereum Block Chain based keen agreement. The assignments in the occasion were transmitted to the understudies in Turkey by means of utilizing test module of the Moodle Learning Management System. For this examination, initial a brilliant agreement was created in which the declaration data could be put away on the Ethereum blockchain and could be check for control purposes if essential. At that point the authentication module created by the scientist in 2014 which uses square structure in the Moodle Learning Management System was refreshed and afterward furnished to work as per the brilliant agreement in theEthereum blockchain. Lakhs of individuals getting Degrees a seemingly endless amount oftime after year, because of the absence of successful enemy of fashion instrument, occasionsthat cause the graduation declaration to be manufactured regularly get took note. So as to take care of the issue of forging authentications, the computerized endorsement frameworkdependent on square chain innovation. All the criminal operations filled against an individual and all the exercises are refreshed in the Personal ID. Utilizing the adjustment procedure we would screen the degree cortication alone as well as whole character and social exercises of that individual. Priya R et al [5] convey Unique based checking utilizingthis framework. Blockchain innovation has developed from being an unchanging record ofexchanges for cryptographic forms of money to a programmable intelligent condition for building conveyed dependable applications. In spite of the fact that, blockchain innovationhas been utilized to address different difficulties, to creator's information none of the past work concentrated on utilizing blockchain to build up a safe and changeless logical information provenance the executives system that consequently confirms the provenance records. In [6], Aravind Ramachandran et al influence blockchain as a stage to encourage reliable information provenance assortment, check and the executives. The created framework uses shrewd agreements and open provenance model (OPM) to record changeless information trails. Creator show that our proposed system can effectively and safely catch and approve provenance information, and forestall any vindictive change to the caught information as long as lion's share

of the members are straightforward The Mainreason for paper [7] is to build up a hypothetical structure for blockchain. Our point is to recognize the hindrances and principle drivers of computerized development and investigate the conceivable outcomes of utilizations of blockchain. A contextual investigation approach is applied: the Norwegian seaward industry. Essential information is gathered through the meetings and auxiliary information is gathered from reports of businesses and organizations, the Internet, and national and global media reports. We havefound that intensions of cost decrease, and the measure of enormous information that sea organizations should process, alongside the successful work intension, are the principle drivers of advanced development. Then again, the terrible nature of web, significant expense usage, the innovation situated culture, the absence of speculation activities, and hazard avoidance are the principle boundaries. A portion of the hindrances and thought processes of advanced development and the prologue to blockchain innovation were calledattention to by before considers. Nevertheless, we have recognized numerous interesting drivers and hindrances explicit to the business. At last, the structure of blockchain process created. One of the examinations prescribes distinctive Learning Management Systems (LMS), Learning Record Stores (LRS), a square chain-based methodology for interfacing learning information among foundation and associations. Subsequently, it is attempted to exploit the blockchain innovation's capacity to give consistency, ease of use, changelessness, security, protection and access control of learning information. The highlights of the proposed framework can be recorded as follows: "Appropriated Consensusand Immutableness"; "Brilliant Contract Based Privacy, Security and Access Control" and"Single Ledger, Multiple Participants [8].

3. Proposed Methodology

A blockchain, initially square chain, is a consistently developing rundown of records, called squares, which are connected and verified utilizing cryptography. Each square regularly contains a cryptographic hash of the past square, a timestamp and exchange information. By structure, a blockchain is intrinsically impervious to change of the information. It is "an open, appropriated record that can record exchanges between two gatherings productively and in an undeniable and lasting manner". Blockchain is a decentralized record used to safely trade computerized money, perform arrangements and exchanges and oversaw by distributed systems. All hubs follow same convention for internode correspondence and approving new squares. When information is approved in any square, it cannot be adjusted by any square. To change specific square information all ensuing square information ought to be adjusted that will bring about intrigue of the systemand all hubs will dismiss that exchange. Online records may not be state-of-the-art or havemissing data. The blockchain innovation may have the option to tackle these issues by giving another approach to store advanced endorsements.

4.1. Proposed Architecture

Right now, blockchain endorsement framework was created dependent on pertinent innovation. The framework's application was modified on the Ethereum stage and is controlled by the EVM. In the framework, three gatherings of clients are included. Schoolsor accreditation units award authentications, approach the framework, and can peruse the framework database. At the point when understudies satisfied certain prerequisites, the specialists award an authentication through the framework. After the understudies have gotten their testament, they can ask about any declaration they have picked up. The specialist co-op is liable for framework support.

Blockchain is a decentralized circulated database. The working procedures of the framework created right now as follows:

•Student will go to their portal and add marks, after that he will get an encoded string of those marks. Once he got that string, he will go to dashboard section where he will get his public and private key. There is upload marks section where student will enter his public and private key along with recipient’s public key and upload marks string.

• After receiving marks digital certificate (encoded string) from student, company need to check whether it is valid or forged. For that, company will send verification request to college along with their public key.

• College (Employee from college who is managing it) will go to their portal and add marksof student, after that he will get an encoded string of those marks. Once he got that string,

he will go to dashboard section where he will get his public and private key. There is upload marks section where he will enter college's public and private key along with recipient's public key and upload marks string.

•Now company have digital certificates from both student and college. They will check and compare both certificates. If both are same then they will approve it. Moreover, if student enters wrong data then his digital certificate will be rejected.

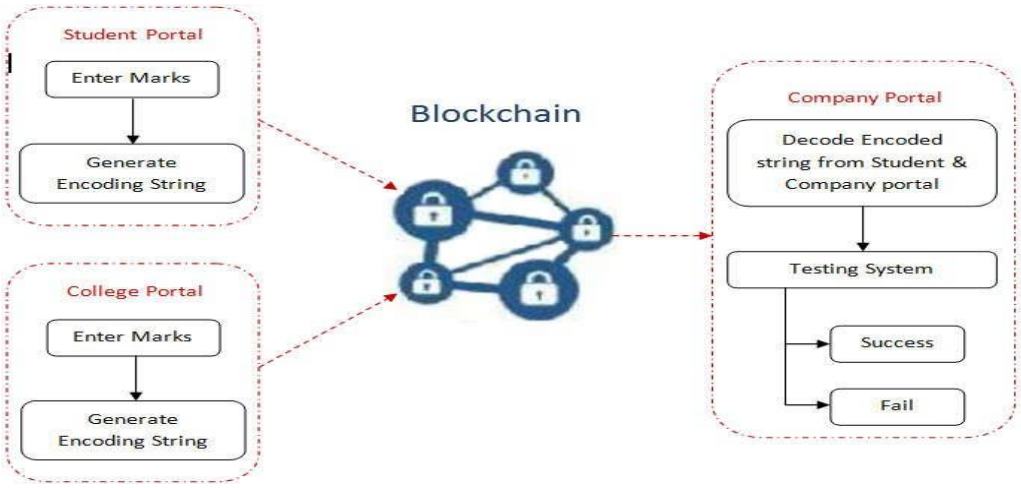

Figure 1: System Architecture

4.2 Objective

To design Blockchain and Smart system which accepts encrypted marks from student, college, and then check its authenticity

4.3 Algorithm

Since its 2008 appearance as a foundation of the cryptographic money Bitcoin, theblockchain innovation increased across the board consideration as a methodology to safelyapprove and store data without a confided in outsider. Blockchain is a decentralized exchange and information the board innovation grew first for Bitcoin digital currency. Blockchain highlights a decentralized and ethical database that has high potential for an assorted scope of employments. A blockchain, initially square chain, is a constantlydeveloping rundown of records, called squares, which are connected and verified utilizingcryptography. Each square commonly contains a cryptographic hash of the past square, a timestamp and exchange information. By plan, a blockchain is innately impervious to change of the information. It is "an open, appropriated record that can record exchanges between two gatherings productively and in an evident and perpetual manner". Blockchainis a decentralized record used to safely trade advanced money, perform arrangements and exchanges and oversaw by distributed systems. All hubs follow same convention for

internode correspondence and approving new squares. When information is approved in any square it can't be changed by any square. To modify specific square information all

ensuing square information ought to be adjusted that will bring about plot of the system andthat exchange will be dismissed by all hubs. In 2008, Satoshi Nakamoto imagined the blockchain for the utilization of digital currency and Bitcoin was its first execution. Bitcoinwas the first open exchange record. The innovation of this cash tackled the twofold spending issue without the need of an outsider. After that other cryptographic money weredesigned on same idea. So, a blockchain is a disseminated database that contains a rundownof records (information). Circulated implies that as opposed to being put away on a focal gadget some place, the whole database is effectively synchronized and put away on a lot ofdifferent gadgets. This is known as a distributed system, much like how Napster was a distributed system for sharing music records. The primary bit of leeway this innovation gives is its capacity to trade exchanges without depending on confided in outsider elements of any methods. It can likewise give information respectability, in-manufactured validness and client straightforwardness. Obstructs: A square contains set of substantial exchanges that are in hash structure and make a Merkle Tree. Each square normally contains a hash pointer as a connect to a past square, a timestamp and exchange information. By structure,blockchains are naturally impervious to alteration of the information. This connecting structures a square of chain. This procedure is iterative and that affirms that past square is dependable and right. Right now can return to beginning square Square time: In blockchainsquare time alludes to when system can make 1 more square in the chain. It time shift fromblockchain to blockchain some blockchain permits new square as often as possible as like clockwork. This time additionally remember the ideal opportunity for which information gets evident. In digital currency term shorter square time implies quicker exchange. In Ethereum Blockchain Block time is inexact 14~15 seconds, while for Bitcoin is approx 10minutes. Decentralization: Blocks are put away in various areas (hubs) so blockchain dispenses with various dangers which comes if information is in single area/stockpiling. In which we don‟t have no essential issue of disappointment. . Information put away on the blockchain is commonly viewed as morally sound, while brought together information is all the more handily controlled, data and information control are conceivable Blockchain Working: Blockchain can be considered as the "Web of significant worth". On the Internet,anybody can compose information and others can understand it. As far as digital currency Keys fills the job of recording the exchange, which is customarily done by banks. It likewisefills a subsequent job, building up trust and character, on the grounds that nobody can altera blockchain. The significant capacities did by banks confirming characters to forestall misrepresentation and afterward recording genuine exchanges - can be completed by a blockchain all the more rapidly and precisely. Square requests in a Blockchain can be considered as a book where, Blocks in a chain = pages in a book.

4. Outcomes

Block chain is protected using encrypted marks string. Hacker can alter encrypted in veryrare case but the decryption of marks string will be very tough part for him. The result of passed marks from student and college portal is encrypted marks string as shown in figure2 and 3 respectively.

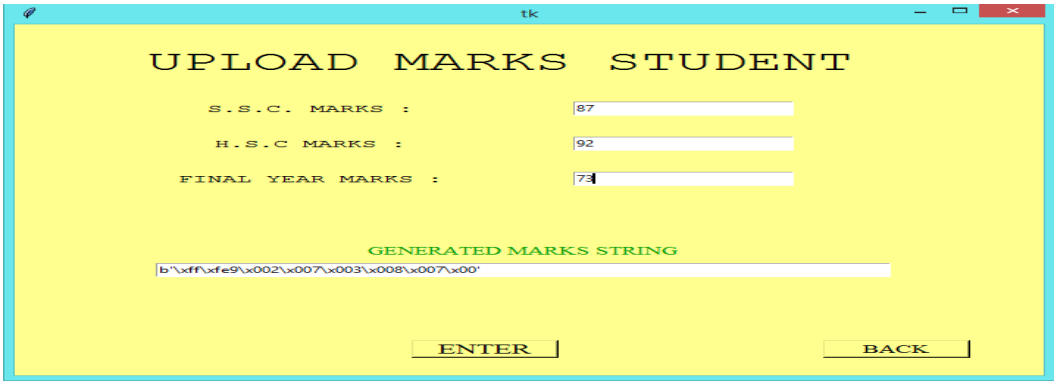

Figure 2: Generation of encrypted marks string from student portal

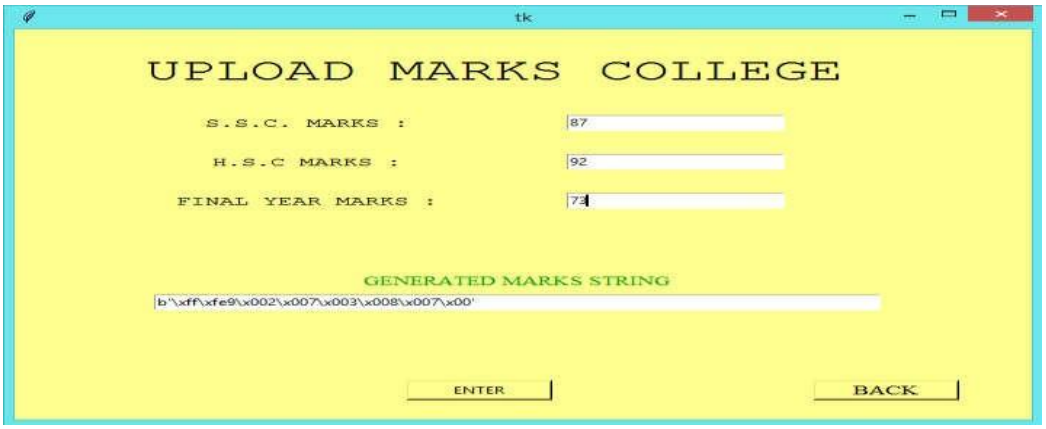

Figure 3: Generation of encrypted marks string from college portal

By using private and public key marks get uploaded to the blockchain which looks like figure 4.

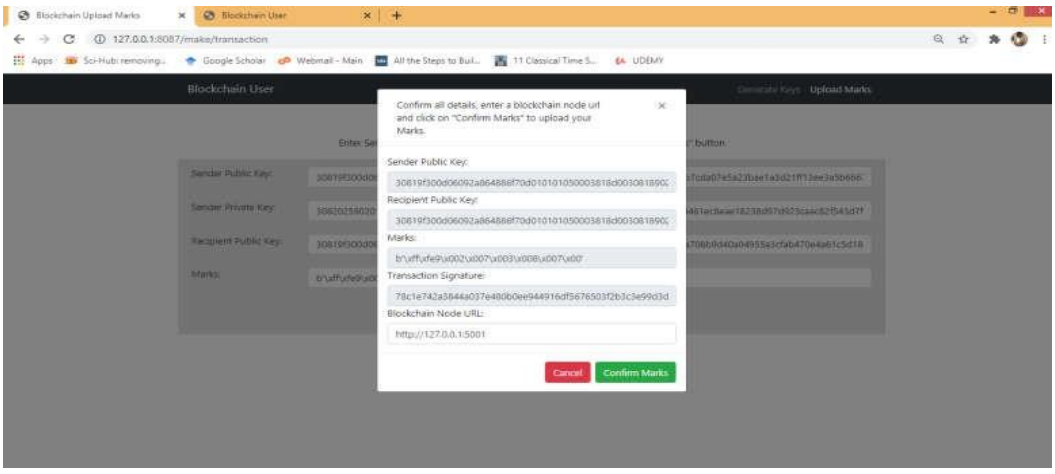

Figure 4: Upload encrypted marks string to block chain

Figure 5 gives brief idea about block chain dashboard. It contains all the necessary information about all the traffic.

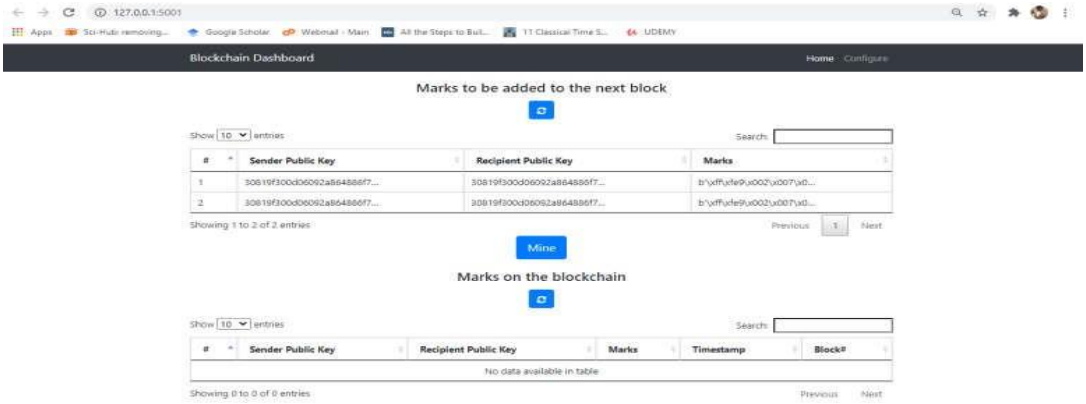

Figure 5: Block chain dashboard

Finally, all the data from blockchain are retrieved from blockchain to the company portal and authentication done. Both the results of authentication are presented in figure 6 and 7.

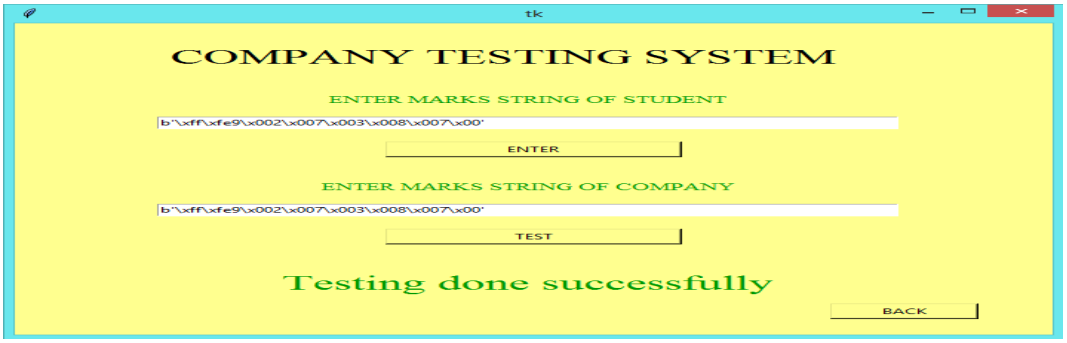

Figure 6: Company testing portal (authentication success)

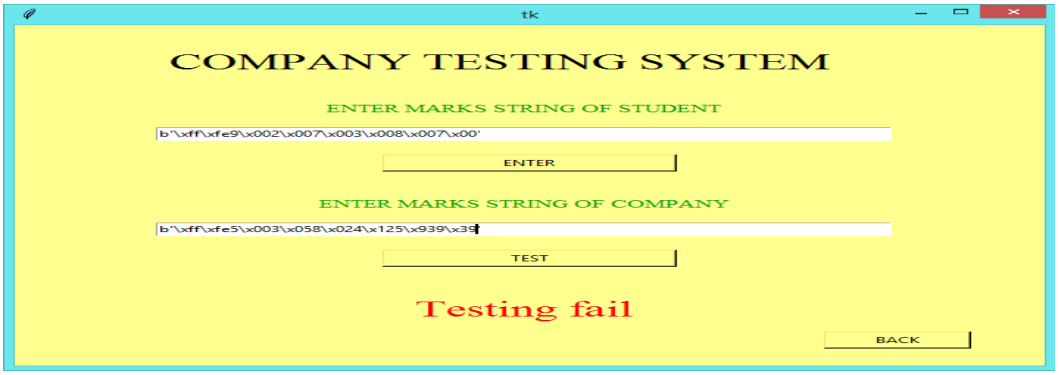

Figure 7: Company testing portal (authentication fail).

5. Conclusion

Proposed system provides additional security to the blockchain technology. If number of nodes are less then proposed system provides excellent accuracy as blockchain fails to

provide good accuracy while having a smaller number of nodes. The results analysis shows that the online verification of the documents becomes more secure and reliable system for document verification can be implemented with the proposed approach of authentication of digital document.

REFERENCES

[1] Jiin-Chiou Cheng, Narn-Yih Lee, Chien Chi, and Yi-Hua Chen, “Blockchain and Smart Contract for Digital Certificate”, Proceedings of IEEE International Conference on Applied System Innovation 2018 IEEE ICASI 2018- Meen, Prior & Lam (Eds)

[2] Neethu Gopal1, Vani V, “Survey on Blockchain Based Digital Certificate System”, International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056 Volume: 05 Issue: 11 | Nov 2018 www.irjet.net p-ISSN: 2395- 0072 © 2018, IRJET | Impact Factor value: 7.211 | ISO 9001:2008 Certified Journal | Page 1244

[3] Yao, Hailong & Wang, Caifen. (2018). A Novel Blockchain-Based Authenticated Key Exchange Protocol and Its Applications. 609-614. 10.1109/DSC.2018.00097. Erinç KARATAŞ, “Blockchain-Based Document Verification Smart Contract for Moodle Learning Management System”, International Journal of InformaticsTechnologies, Volume 11, Issue 4, October 2018 399 Developing Ethereum

[4] Jiin-Chiou, Narn-Yih Lee, Chien Chi, YI-Hua Chen, Blockchain and Smart Contract for Digital Certificate, Proceedings of IEEE International Conference on Applied System Innovation 2018

[5] Aravind Ramachandran Dr.Murat Kantarcioglu “Using Blockchain and smart contracts for secure data provenance management”, arXiv:1709.10000v1 [cs.CR] 28 Sep 2017

[6] T. Keerthana1 , R. Tejaswini2 , V. Yamini3 , K. Hemapriya “Integration of Digital Certificate Blockchain and Overall Behavioural Analysis using QR and Smart Contract”, International Journal of Research in Engineering, Science and Management Volume-2, Issue-3, March-2019

[7] Ocheja, P., Flanagan, B., & Ogata, H, “Connecting decentralized learning records: a blockchain based learning analytics platform”, In Proceedings of the 8th International Conference on Learning Analytics and Knowledge (pp. 265- 269). ACM

[8] Duan, B., Zhong, Y., & Liu, D, “Education application of blockchain technology: learning outcome and metadiploma” In Parallel and Distributed Systems (ICPADS), 2017 IEEE 23rd International Conference on (pp. 814-817). IEEE.

[9] 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

[10] Zibin Zheng , Shaoan Xie, Hong-Ning Dai, Xiangping Chen , ” An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends”, IEEE 6th International Congress on Big Data, 2017

[11] M. J. M. Chowdhury, A. Colman, M. A. Kabir, J. Han and P. Sarda, "Blockchain Versus Database: A Critical Analysis", 2018 17th IEEE International Conference On Trust Security And Privacy In Computing

[12] Beck Roman, Czepluch Jacob, Lollike Nikolaj and Malone Simon, "Blockchain - The Gateway To Trust -Free Cryptographic Transactions", *Research Papers*, no. 153, 2016