ISSN: 0369-8963

A Trustworthy Platform for Safeguarding and Validating Educational Credentials using Blockchain Technology

DR. P. C. SENTHIL MAHESH
Associate Professor,
Department of Computer Science and Engineering,
Excel Engineering College, Namakkal, Tamilnadu, India.

DR. K. MUTHUMANICKAM
Professor, Kongunadu College of Engineering and Technology,
Department of Information Technology, Tiruchirappalli, Tamilnadu, India

Abstract:

In one way or another, education serves as the soul of society growth. Aspirants who earn their degrees honestly will use their knowledge and abilities to benefit society. While the number of universities and graduates continues to rise year after year, the need to simply validate degree credentials creates new business prospects. Students seek a low-cost, easy-to-understand evidence of certification, while companies demand quick and reliable verification of degrees when hiring. Because a large number of students graduate each year, the issue of fake credentials could become a major problem. In this case, an overlay method based on blockchain technology is used to keep legitimate certificates in digital form and quickly verify them when needed. The proposed approach ensures that the certifications, once verified, are available in an irretrievable form for immediate verification with future reference and that the existing certification system is kept tamperproof. A prototype of a blockchain-based credential security and verification system is constructed in the Ethereum test network to confirm the legitimacy of the suggested method. The results of the implementation and testing reveal that it is a safe, secure and practical solution for online credential management.

Keywords: *Blockchain, Document Verification, Digital Certificate, distributed, Preprocessing.*

INTRODUTION

The basic pattern of a student's education in India is as follows: admittance to preschool, then constant changes in faculty for primary, secondary, and high school studies. Students who have completed high school must now apply for college entrance. In addition, there is a constant rotation of instructors for graduation. This is frequently the basic cycle for a student's academic years. Some pupil continues their education after that. As a result, the disadvantage of this cycle is that a student must submit all of his/her certificates for validation at each level. The certificate may be lost or damaged as a result of this. It's also time-consuming for the validator to show each certificate. According to survey of All India Higher Education 2019-20 [1], in recent years with around 93 lakh students graduating each year as shown in Figure 1 which is extremely difficult to keep track of and validate such a big number of records.

Associate degree undesirable state of affairs, such as change of state and the manufacture of fake or duplicate certificates, is on the rise. Fake universities are issuing certifications, as well as forged certificates from existing trustworthy universities. This phoney credential problem has become a pain in the neck for both colleges and recruiting businesses as a result of centralization and digitization, and it requires a swift response. Since technology has progressed so far, distinguishing

 https://doi.org/10.37896/pd91.5/91566

ISSN: 0369-8963

between a portend and an inventive certificate would need a great deal of focus and result in the waste of valuable time and financial loss.

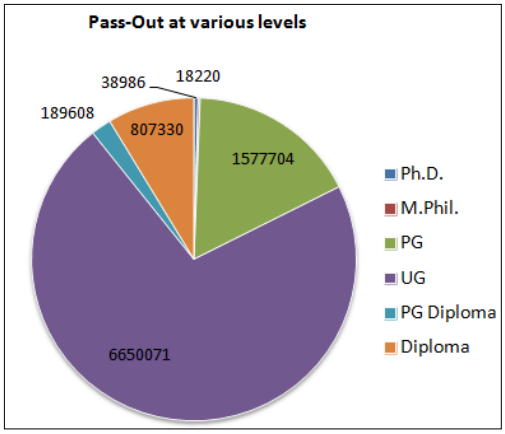

Fig.1 Pass out at different levels during 2020-21 in India

Blockchain technology becomes a suitable choice to create a decentralized application which is capable of maintaining all data secure and tamper-proof. The data is saved in text format in this application to make development and testing easier, but once a particular transaction is ended, the data is transformed to hash values and stored in a block across the entire network. Because numerous copies are spread in the peer network, a single bit of change in a specific block should corrupt many of the data in the chain completely, which is not conceivable. As a result, the data's integrity is preserved. Ethereum test net is used to implement and test the proposed technique. When data is about to be stored as an Ethereum blockchain, the administrator's intervention is reduced. It is held in an account and distributed around the network as a recompense for a miner whose system serves as the block's data carrier.

In Existing system, the problem of fake certificates is a big issue. Companies hiring thousands of freshers spend large amount of money to get the educational certificates and transcripts verified of applicants. To address this problem, we have proposed an idea of digital certificate system for verification of educational certificates using blockchain technology.

CONTRIBUTIONS AND PAPER ORGANIZATION

From the existing system, we have found several research gaps. Hence, a mechanism is needed to develop a more robust, and authentic framework for validating the legitimacy of educational information like school certificate, degree certificate of a student or employee through reliable platform.

- The mechanism that takes lower computational cost.
- Trust based authentication approach is needed to ensure the legitimacy of educational certificates.
- The proposed protocol is implemented in real-time and its robustness has been verified.

https://doi.org/10.37896/pd91.5/91566

ISSN: 0369-8963

The rest of the paper is discussed as follows. The review of related published research is described in Section 2. Section 3 elaborated the present certificate verification system. The proposed blockchain technology-based certificate verification method is described in Section 4. Section 5 discussed about the simulation, findings and discussions. The article is concluded in Section 6.

RELATED WORKS

Nowadays the students achieve various educational certificates. Student produces these certificates while applying for jobs at public or private sectors, where all these certificates are needed to be verified manually. There can be incidents where students may produce the fake certificate and it is difficult to identify them. This problem of fake academic certificates has been a longstanding issue in the academic community. Because it is possible to create such certificates at low cost and the process to verify them is very complex, as they are manually needed to be verified. This problem can be solved by storing the digital certificates on the Blockchain.

Khan et al. [2] proposed a hyperledger-based architecture for validating the legitimacy of degree certificates and providing a traceable path between two parties, such as a university and a third party wishing to verify the authenticity of a student's or person's certificate. Harer et al. [3] used the ADOxx concept to develop a decentralized mechanism for certificate verification. This method is appropriate for Ethereum-based system applications and aids in the verification of certificate transparency and immutability. The difficulty is in obtaining permission, as well as the encryption algorithm employed, the network model used, and so on.

Bhumichitr et al. [4] investigated how blockchain technology can aid in the verification of proven academic credentials. Despite the fact that this solution employed Ethereum and was modified for the public network, it failed to leverage Hyperledger and had insufficient data for user presentation. Fedorova et al. [5] explored the influence of blockchain technology in the educational sphere in order to check the authenticity of certificates issued by a university or educational institution. A case study is sometimes used for demonstration purposes. However, excluding the heperledger architecture increases the complexity or expense of computing. Lizcano et al. [6] looked at how to use blockchain technology to manage the registration, transaction, and legalization of educational data on an institution's staff. This strategy aids in providing a replica of learning that can be trusted everywhere. It, on the other hand, failed to emphasize the use of intangible modular structural design.

Educational degree verification traceability reliant blockchain applications are based on permissioned trust relationships, inherent stakeholder interest in the stated consensus policy, and do not require the use of a proof-of-work algorithm [7]. Nothing will be removed or changed if the common system's duplication is maintained and the data is recorded. The digital ledger's copy, however, is matching to the previous ledgers in the network. Different hyperledgers exist, each with a specific role in a different enterprise setting. Turkanovi et al. [8] proposed a solution in the shape of an architecture reference model that allows businesses and government agencies to take advantage of blockchain technology by combining electronic signature scheme with blockchain technology.

 https://doi.org/10.37896/pd91.5/91566

ISSN: 0369-8963

Three popular blockchain systems namely, Hyperledger Fabric, Hyperledger Iroha and Ethereum were evaluated as test beds for developing a system with the fundamental functionalities required for reliable degree verification [9]. Hyperledger Iroha was employed in the approach and system developed and presented in this article, demonstrating that this platform can be flexible to straightforwardly develop decentralized applications. The fabric is an extensible blockchain solution that enables developers to maintain a distributed digital ledger [10] through the appropriate execution and flow of functioning of digital indenture of higher educational degree attestation, traceability and verification using recent blockchain security measures.

In the private ledger network architecture, the HEC authority must consider, design, and develop distinct educational policies and pathways regarding blockchain technology reliant hyperledger fabric smart agreement implications like digital record, maintainability, decentralized storage preservation, and stakeholder changes permission, as well as rights of consensus [11]. The HEC should work with an university and other local sectors to make manual degree attestation verification easier. The main goal of blockchain is to safeguard essential data organizations and to satisfy the specific type of data that will be saved on the digital ledger using blockchain technology, as well as the storage processes, like on- and off-chain information protection storage [12]. The whole data in the higher educational degree verification is more sensitive and secret; as a result, the data must be stored and checked against and investigated the on-chain hashes.

Forgery of certificates has long been a concern in Egypt's academic sector [13]. It is now usual to obtain a false certificate claiming graduation from a public or private university in order to apply for employment more easily and be deemed as skilled as someone with a legitimate degree. Blockchain technology which is recognized for its dependability and trustworthiness is being used to solve this problem. As a response to the counterfeit problem, the suggested system attempts to create digital degree certificates specifically for higher education in Egypt. This suggested system allows companies and institutions to track a student's certifications, allowing them to validate the certificates earned.

An overlay method based on blockchain technology is suggested [14] to keep legitimate certificates in digital form and quickly verify them when needed. The proposed approach ensures that the certifications, once verified, are available in an irretrievable form for immediate verification with future reference and that the existing certification system is kept tamperproof. A prototype of a blockchain-based credential security and verification system is constructed in the Ethereum test network to confirm the legitimacy of the suggested method.

Ming et al. [15] introduced CrowdBC, a blockchain-based decentralized crowd sourcing framework in which a requester's task may be done by a set of employees without the need for a third party, users' anonymity can be ensured, and the needed transaction cost is cheap. Haibo Yi et al. [16] suggested a blockchain-based e-voting system that fits the e-voting procedure's basic requirements. In a blockchain, hash values are used to link all votes. Yi Chen et al. [17] devised a storage method that combines blockchain and cloud storage to stockpile and administer personal clinical data. Ali Dorr [18] presented a blockchain reliant framework to preserve users' privacy and increase the vehicle ecosystem's security.

Xiao Yue et al. [19] proposed a blockchain-based healthcare data gateway that allows patients to control and share their medical reports seamlessly and securely without infringing on their privacy, as well as providing a innovative method to enhance the quality of healthcare medical systems

 https://doi.org/10.37896/pd91.5/91566

ISSN: 0369-8963

whilst maintaining patient clinical data confidential. Daniel Kraft et al. [20] defined mining in the form of a poison progression through time reliant intensity, and he utilized this model to forecast block durations for different hash-rate scenarios. Tomaso Aste et al. [12] wrote a paper outlining the fundamentals of blockchain technology, as well as the obstacles, future potential, and expected influence of technologies like distributed ledger and blockchain on industry and society.

In this manuscript, we propose a certificate generation and verification system based on blockchain technology. Our system also uses a build signature scheme, which helps to achieve anonymity of the users without using mix nets or trusting a third party. Moreover, due to the nature of the blockchain, the data remains indefinitely and unchanged, which also make audit procedures much easier.

EXISTING SYSTEM

Mark memos are now distributed as a printed copy to students under the current arrangement. There is no method to check the certificate digitally. There will be no link between the students, the institution, and the certificate once it is handed to the students.

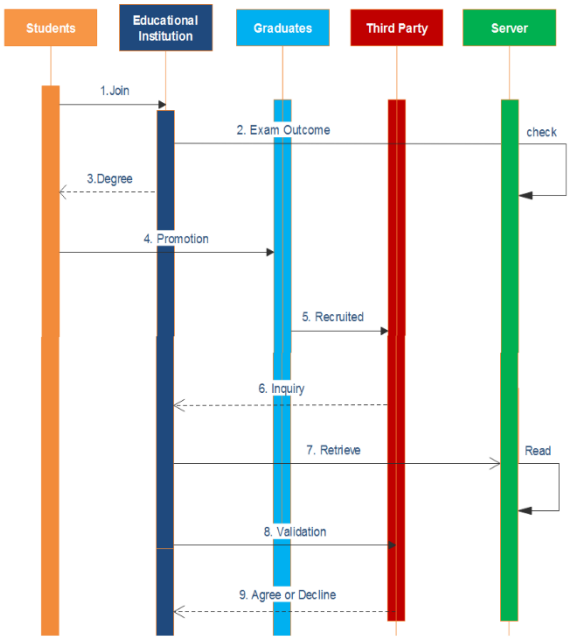

Fig.2 Existing method for certificate verification

There is no mechanism for securely storing certificates and verifying them when needed. As a result, for backdoor jobs, phoney degree certificates are generated. Industries require a background check of an employee's educational details when they are hired, and this verification is done manually by a team or by a third party. There may be a delay in the procedure, giving you the opportunity to handle the university or college's concerned department personnel who entertain the verification call. It's considerably more difficult to tell the difference between a fake and a real degree if the root register has previously been tampered with. Some colleges keep certificates in digital form, but they are also connected to a centralized network, making them vulnerable to tampering. As a result, there may be a rise in incidents of fraud because there are no safeguards in

 https://doi.org/10.37896/pd91.5/91566

ISSN: 0369-8963

place to ensure the security of data, both in manual and digital formats. The lack of a timestamp facility and a way of keeping records at a central database are the main causes of this difficulty. Figure 2 depicts the current system, which begins with a student's acceptance and ends with an employer's verification of a graduate's credentials. The following are the different stages:

i. When students join to an educational institution or graduate school are referred to as "joining" or "admitting."
ii. Examination results of the end-semester or year-end are kept in a central server.
iii. Original degree certificate is issued including mark statements on paper.
iv. The students have now been transformed into graduates with a degree.
v. Recruiters or employers provide graduates with acceptable career opportunities.
vi. Employers ask universities to verify an employee's credentials.
vii. Universities verify data by retrieving it from a central database server.
viii. Check the given data against the retrieved data to ensure its legitimacy before confirmation sent to the third party.
ix. It is decided based on the report, confirm or decline the graduate's assignment.

OUR PROPOSED SYSTEM

Because the institution, students, and businesses are concerned about certificate storage and security, the proposed solution uses blockchain technology to store and verify student credentials. When a certificate is added to a block, it returns a unique certificate number as well as a main key of the student register number. The student can validate the certificate and the company can verify if the certificate supplied by the student or employee is permitted or not using the unique certificate ID. Aside from that, each student will have a register number and date of birth, which will allow the verifier to easily access all of the certificates listed in the same person's name to validate individually

To create the blockchain based unmodifiable certificates, initially the university needs to get registered. Any transaction can be sent through the wallet address of the registered university. Only the owner of the smart contract has the authority to add the universities. Once added the university, will be able to access the system and can create certificates with data fields. Each created certificate will be stored in the Inter planetary file system (IPFS). The architecture of the proposed method is shown in Figure 3.

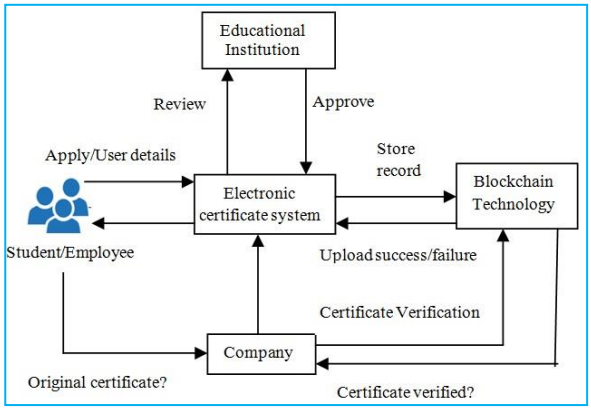

Fig.3 Architecture of the proposed method

https://doi.org/10.37896/pd91.5/91566

ISSN: 0369-8963

It will then return the unique hash generated using the (secure hash algorithm) SHA-256 algorithm. This will serve as a unique identity for each document. This generated hash and details of certificates will be stored in the blockchain and the student will be provided with the resultant transaction id. Anyone can use this transaction id to verify the certificate details and can view the original copy of the certificate using the IPFS hash stored along with the data. And it is not possible to modify this certificate or to create a fake certificate using the same data. Hence, with this, we can solve the problem of certificate forgery. The important components of single block are shown in figure 4. The fields are chosen to incorporate the relevant information and may change depending on the needs.

1: Pseudo random number: It is the miner adds a random value to the hash problem to solve it.
2: Register number and date of birth are the candidate's identification number.
3: Degree Certificate: Vital information like the student's name, register number, certificate number, issuing date, and unique ID of the controller of exam where the certificate is issued are entered in its plain format.
4: Time stamp – It denotes the actual date with time of a block's creation.
5: Hash value: It is the previous block's cryptographic hash value, calculated using SHA-256, is used to connect the new block with the active chain.

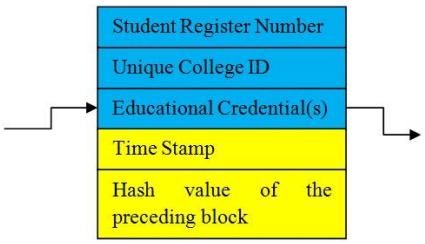

Fig.4 Components of a single block

EXPERIMENTAL OUTCOME AND DISCUSSIONS

The proposed system is implemented and tested by using the following softwares: JavaScript, Truffle, Solidity, Ganache, Ethereum, and Chrome extension Metamask. Ganache is part of the Truffle ecosystem. Ganache is used for the development of DAPP (distributed application, a blockchain) and once it is developed and tested on ganache, it can be deployed on ethereum client like geth or parity. Truffle helps to develop, test, and deploy the DAPP. Metamask is one of the digital currency wallets to store and transact on ethereum using ethereum based tokens.

Usually, certificate authorities generate and attach blocks to the blockchain, and copies of the blockchain are circulated to peer nodes of the appropriate universities and autonomous colleges. Every entry will be assigned a unique transaction identifier when they are added to the blockchain, which may be used in conjunction with his register number to obtain or validate data. The verifiers (recruiting company) can use the application to access the blockchain and finish the procedure quickly and reliably, as well as acquire the data of that specific employee identifier. Assume a blockchain is produced over time with few certificates designated as blocks of data, and the copies are circulated throughout the network as mentioned earlier. If an attacker intends to change a

https://doi.org/10.37896/pd91.5/91566

ISSN: 0369-8963

specific block, the hash value of that block will change, and the change will be reflected in subsequent blocks of the blockchain. Even if he was successful in changing the next blocks in one node, the change would not be spread to the other nodes since it is a dispersed network of nodes, as shown in Figure 5, and the alteration would be immediately identifiable while executing the agreement procedure.

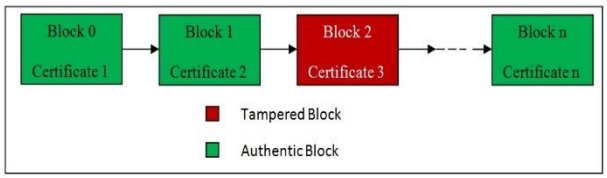

Fig.5 Effect of tampered block in a specific block

The data entry form in Figure 6 collects all of the student's information and provides a certificate amid a unique identifier.

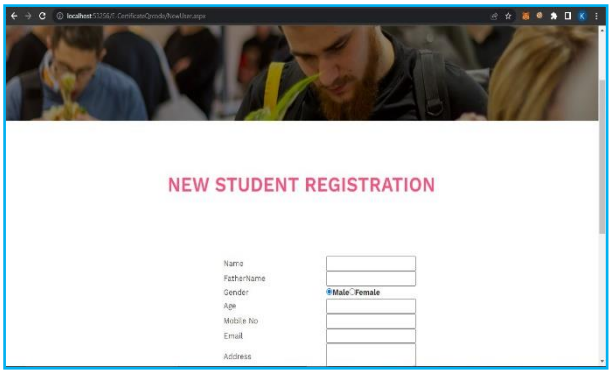

Fig.6 Information collection form

As indicated in Figure 7, the certificate is created. Recruiters or any third party can verify the certificate using its unique information included in the certificate if necessary. To make the testing process easier, the blockchain is established by keeping textual data. There are other more ways to create a blockchain as listed below.

a. Incorporating the hash values of the mark statements.
b. Including the Merkle tree's root which represents a whole batch of student mark statements.

The pros and cons of the aforesaid strategies are not addressed in this paper.

CHALLENGES

Data immutability is one of the main features of blockchain. It serves as a large public ledger where node in network verifies and save the same data. The process of certificate generation is open and transparent system where any organization can verify information of any certificate using this system. In challenges the system helps in eradicating problems of fake certificates.

https://doi.org/10.37896/pd91.5/91566

ISSN: 0369-8963

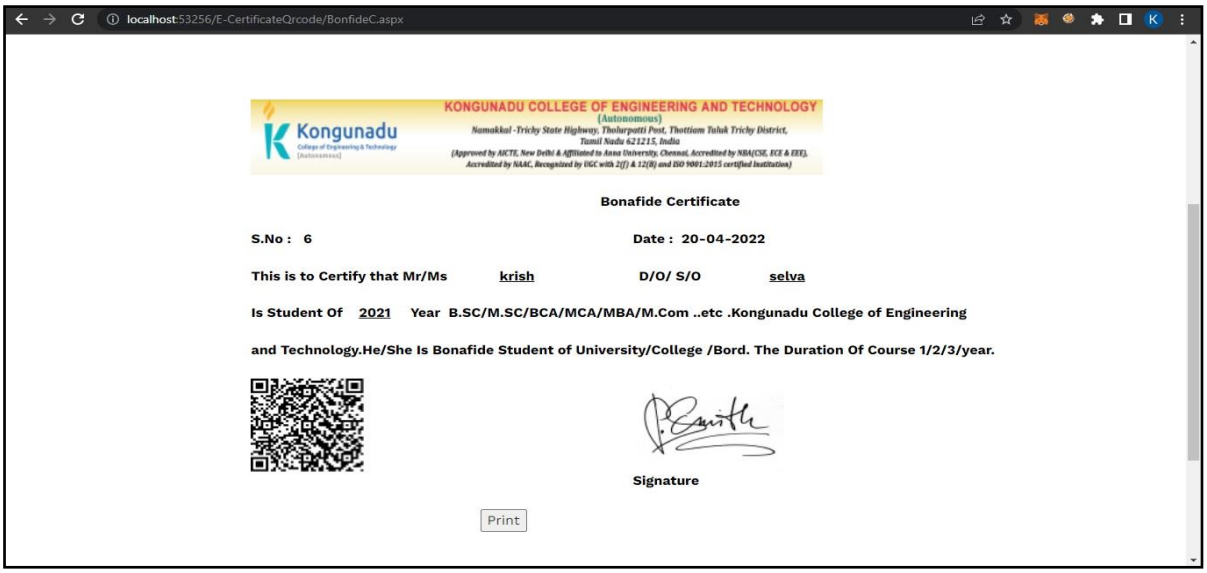

Fig.7 Original Certificate Generation

- This tool provides universities and autonomous institutions with a tamper-proof platform for publishing results and verifying mark memos supplied by students to companies. For the sake of simplicity, the marks are saved in text format in this prototype. If necessary, they can be saved as an image.
- This blockchain is managed by a group of colleges and universities. Students should contact the consortium if they desire to keep their educational data on this permitted site.

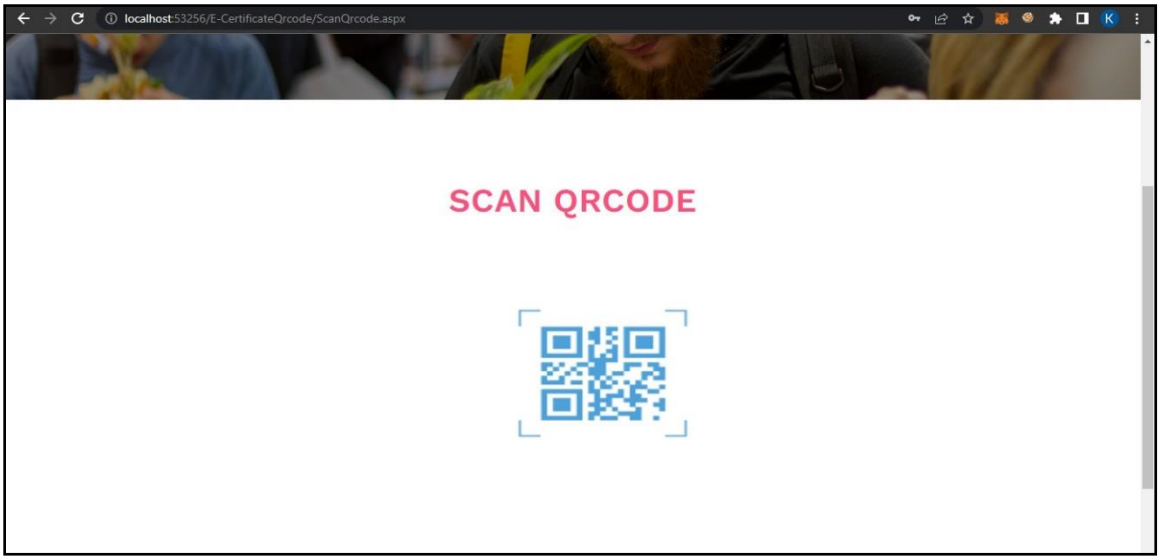

Fig.8 Scanning QR code option

- It is difficult to construct a person's authentic certificate using a replayed attack, which involves changing a single bit in the hash code linked with a genuine certificate generated

https://doi.org/10.37896/pd91.5/91566

ISSN: 0369-8963

before as shown in Figure 9.

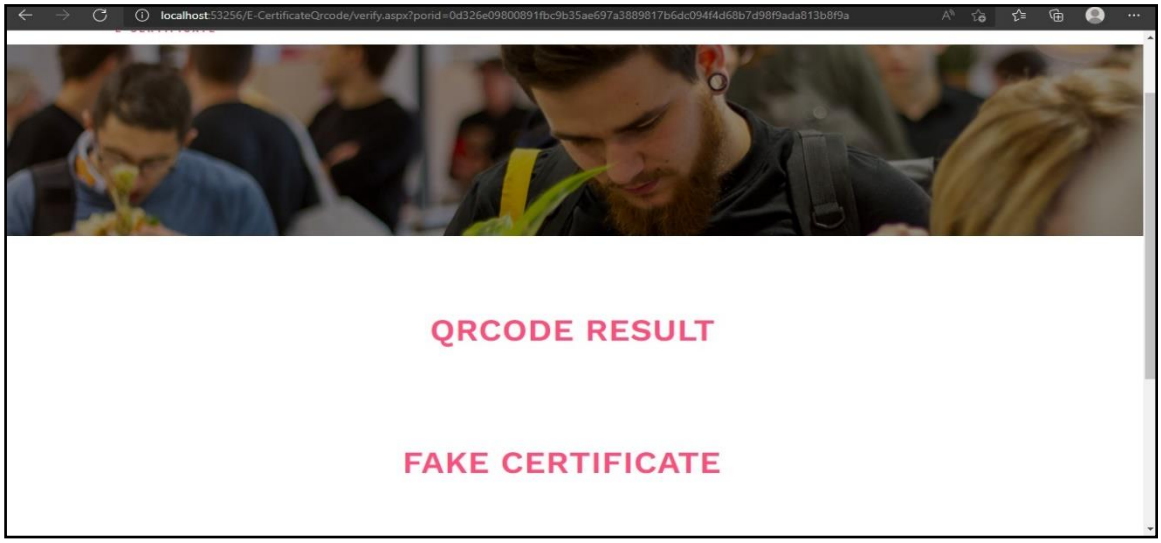

Fig.9 Result of replayed attack

- From X class until graduation/post-graduation, this blockchain reliant distributed ledger is capable of tracking each academic information of the student. Only authorized users have the ability to add marks to the blockchain. Students' credentials are:

a. Added, including their roll number, name, grades, and a unique ID such as a register number.
b. Each of the created certificates has its own certificate ID, which is unique and used during verification.
c. QR code can also be used during certificate verification process as shown in figure 8.

Original hash code of the genuine certificate:
0d326e09800891fbc9b35ae697a3889817b6dc094f4d68b7d99f9ada813b8f9a

Tampered hash code of the genuine certificate:
0d326e09800891fbc9b35ae697a3889817b6dc094f4d68b7d99f9ada913b8f9a

It is inferred from Table 1 that the proposed method incurs minimal execution time for completing each transaction, thus suitable to apply in real-time.

NO. OF NODES	PARAMETER	TIME TAKEN (SECOND)
1	Average time of block generation	0.003
	Delay of confirmation	0.79
	TPS (Number of transactions per second)	230
2	Average time of block generation	0.007

https://doi.org/10.37896/pd91.5/91566

ISSN: 0369-8963

	Delay of confirmation	0.21
	TPS (Number of transactions per second)	590+
4	Average time of block generation	0.0012
	Delay of confirmation	0.03
	TPS (Number of transactions per second)	900+
6	Average time of block generation	0.009
	Delay of confirmation	0.033

Table 1. Efficiency of the proposed method.

CONCLUSIONS

The proposed system is a blockchain consortium between universities, an educational institution and businesses. Universities often add students' certificates first, and then firms or anyone can verify the educational credentials using the student's register number and date of birth. The educational data embedded through a blockchain will be secured; thus nobody can corrupt or insert a new transaction to it. The certificates are afterwards verified using the unique identifier to be generated for each transaction. This method can be used by any university or institution to give additional protection for certificates and student information. The proposed system, cuts down the management cost, prevents document forgery and provides accurate and reliable information on digital certificates. Fake certificates can be eliminated, and there will be no need for them to be validated. This can be extended in the future to guarantee integrity to any sort of document, not just in the education sector, but also in government sectors that require a digital document time stamp.

The entire project of the proposed scheme is available in GitHub: https://github.com/kiranselva/CollegeCertificate.

REFERENCES:

[1] All India Survey on Higher Education. Accessed on March 15, 2022. Available: https://www.education.gov.in/sites/upload_files/mhrd/files/statistics-new/aishe_eng.pdf

[2] Khan A.A., Laghari A.A, Shaikh A.A., Bourouis S., Mamlouk A.M., Alshazly H., “Educational Blockchain: A Secure Degree Attestation and Verification Traceability Architecture for Higher Education Commission,” Applied Science, vol. 11, pp. 1-22. 2021.

 https://doi.org/10.37896/pd91.5/91566

ISSN: 0369-8963

[3] Härer F., Fill H.G., “Decentralized attestation of conceptual models using the Ethereum blockchain,” Proceedings of the 2019 IEEE 21st Conference on Business Informatics (CBI), Russia, vol. 1, pp. 104–113, 2019.

[4] Bhumichitr K., Channarukul S., AcaChain, “Academic Credential Attestation System using Blockchain,“ Proceedings of the 11th International Conference on Advances in Information Technology, Thailand, pp. 1–8, 2020.

[5] Fedorova E.P., Skobleva E.I., “Application of Blockchain Technology in Higher Education, “European Journal of Contemporary Education. vol. 9, pp. 552–571, 2020.

[6] Lizcano D., Lara J.A., White B., “Aljawarneh, S. Blockchain-based approach to create a model of trust in open and ubiquitous higher education. Journal of Computing in Higher Education, vol. 32, pp. 109–134, 2020.

[7] Xu X., Sun G., Luo L., Cao H., Yu H., Vasilakos A.V., “Latency performance modeling and analysis for hyperledger fabric blockchain network,” Information Processing & Management, vol. 58, no. 1, pp. 102436, 2021.

[8] Turkanovi´c M., Podgorelec B., “Signing Blockchain Transactions Using Qualified Certificates,” IEEE Internet Computing, vol. 24, pp. 37–43, 2020.

[9] Vlachou V., Kontzinos C., Markaki O., Kokkinakos P., Karakolis V., Psarras J., “Leveraging Hyperledger Iroha for the Issuance and Verification of Higher-Education Certificates,” International Journal of Science Education, vol. 14, pp. 755–763, 2020.

[10] Lu N., Zhang Y., Shi W., Kumari S., Choo K.K.R.,”A secure and scalable data integrity auditing scheme based on hyperledger fabric,” Computer Security, vol. 92, pp. 101741, 2020.

[11] Khan A.A., Uddin M., Shaikh A., Laghari A.A., Rajput A., “MF-Ledger: Blockchain Hyperledger Sawtooth-enabled Novel and Secure Multimedia Chain of Custody Forensic Investigation Architecture,” IEEE Access, vol. 9, pp. 103637–103650, 2021.

 https://doi.org/10.37896/pd91.5/91566

ISSN: 0369-8963

[12] Khan A.A., Shaikh A.A., Cheikhrouhou O., Laghari A.A., Rashid M., Shafiq M., Hamam H., "IMG-forensics: Multimedia enabled information hiding investigation using convolutional neural network," IET Image Processing, pp. 1-9, 2021.

[13] El-Dorry A., Reda M., El Khalek S.A., Mohamed S.E., Mohamed R., Nabil A., "Egyptian Universities Digital Certificate Verification Model Using Blockchain," Proceedings of the 2020 Association for Computing Machinery, Cairo, pp. 79-83, 2020.

[14] Reddy T.R., Prasad Reddy P. V. G. D., Srinivas R., Raghavendran Ch. V., Lalitha R. V. S., Annapurna B., "Proposing a reliable method of securing and verifying the credentials of graduates through blockchain". EURASIP Journal on Information Security, vol. 7(2021), pp. 1-9, 2021.

[15] Li M., "CrowdBC: A Blockchain-Based Decentralized Framework for Crowdsourcing," IEEE Transactions on Parallel and Distributed Systems, vol. 30, no,6, pp. 1251-1266, 2019.

[16] Yi H., "Securing e-voting based on blockchain in P2P network," EURASIP Journal on Wireless Communications and Networking, vol. 137(2019), pp.1-9, 2019.

[17] Chen Y., Ding S., Xu Z., "Blockchain-Based Medical Records Secure Storage and Medical Service Framework," Journal of Medical Systems, vol. 43, no. 1:5, pp. 1-9, 2019.

[18] Dorri A., Steger M., Kanhere S. S., Jurdak R., "BlockChain: A Distributed Solution to Automotive Security and Privacy," IEEE Communications Magazine, vol. 55, no. 12, pp.119-125, 2017.

[19] Yue X., Wang H., Jin D., Li M., Jiang W., "Healthcare data gateways: found healthcare intelligence on blockchain with novel privacy risk control," Journal of Medical Systems, vol. 40, Article 218(2016), pp. 1-8, 2016.

[20] Kraft D., "Difficulty control for blockchain-based consensus systems," Peer-to-Peer Networking and Applications, vol. 9, pp. 397-413, 2016.

 https://doi.org/10.37896/pd91.5/91566

ISSN: 0369-8963

[21] Aste T., Tasca P., Matteo T.D., “Blockchain Technologies: The Foreseeable Impact on Society and Industry,” Computer, vol. 50, no. 9, pp. 18-28, 2017.

[22] Ning J., Cao Z., Dong X., Liang K., Wei L., Choo K.-K.R.., “CryptCloud$^+$+:secure and expressive data access control for cloud storage,” IEEE Transactions on Services Computing. vol. 14, no. 1, pp. 111–124, 2021.

 https://doi.org/10.37896/pd91.5/91566