

See discussions, stats, and author profiles for this publication at: <https://www.researchgate.net/publication/360850030>

Certificate Generation and Verification System Using Blockchain Technology and Quick Response Code

Article in IOSR Journal of Computer Engineering · May 2022

CITATIONS

3

READS

7,591

3 authors, including:



Umar Abdullahi Muhammad

Federal University of Technology Owerri

19 PUBLICATIONS 9 CITATIONS

SEE PROFILE



G.I.O. Aimufua

Nasarawa State University

31 PUBLICATIONS 26 CITATIONS

SEE PROFILE

Certificate Generation and Verification System Using Blockchain Technology and Quick Response Code

Muhammad Umar Abdullahi¹, Dr. G. I.O. Aimufua², and ³Adamu Aminu
Muhammad

^{1, 3, 4} Student, Department of Computer Science, Nasarawa State University, keffi, Nasarawa State, Nigeria.

²Head of Department, Department of Computer Science, Nasarawa State University, Keffi, Nasarawa State, Nigeria

Abstract: The number of certificate counterfeits in our society has become challenging and prevalent. Today, forging certificates has become a business tumbling from the need/want of the people for employment. Graduates with legitimate certificates/degrees are denied job opportunities by the holders of these forged credentials. To address this problem, many researchers have proposed a certificate verification system. Although the existing systems can solve some of the major problems such as accessing student's records with the provision of a central database to manage these records electronically. However, the system can easily be hacked and manipulated since it is mostly available on centralized servers. This dissertation developed a certificate generation and verification system using blockchain technology and Quick Response (QR) code. Iterative and incremental models were used for the system modelling. Also, Data flow diagrams and use case scenarios are used to demonstrate the functionality of the web application. Consequently, suitable programming languages were chosen to implement the proposed algorithm of the system. Hypertext Preprocessor Pages (PHP) and Spring boot (Java framework) were used for the implementation of frontend and backend respectively. The system was evaluated and show that not only is secure but also protects the student's identity by providing an anonymous verification setting.

Keywords: (ABS) Blockchain, IPFS, Certificate, Generation, Verification and Quick Response Code

Date of Submission: 03-02-2022

Date of Acceptance: 16-02-2022

I. Introduction

The internet is an important vehicle backing up the exchange of information among people with huge avenues or platforms for data transmissions. Yet, despite its current scale and latitude, users are still discreet to use it for most businesses (Javier, Javier, Oscar, & Manel, 2004). The issue of security becomes a major concern since one cannot guarantee that the internet is fully secured for all types of transactions. Research reveals that the traditional certificate verification system currently in use in most universities around the world is paper-based that is known with lots of defects. This method of verification is manually done which is ineffective and less efficient for institutions with a variant number of records. Furthermore, educational institutions attempt to eliminate fraud and forgery in numerous ways by adopting different approaches, still, most of the existing methods are time-consuming because they are labour-intensive, partially automated or involve human to human interaction (Osman & Umar, 2016). Verification of certificates is also a major concern for institutions, academic organizations and employers or recruiters. Employers have been experiencing a high alarming rate of fake certificates (Musee, 2015). This problem warrants the need for a secured online certificate generation and verification system with little or no human intervention. A certificate generation and verification system is an application system used to create scrolls or certificates (Patrick, Karim, & Kenneth, 2018). They further explained that it is a computerized method of authenticating and validating claims of certificate ownership made by someone from an institution. Regrettably, several approaches that were adopted to combat this menace have proven futile and haven't been measured up with modern techniques deployed in academic fraud. Blockchain technology has emerged as an important mechanism for tamper-proof digital records and is fast becoming applicable in several industries and institutions. Xu et al. (2021) described blockchain technology as a decentralized communication and data management solution that is growing and has no room for a trusted third party. Devoid of a centralized authority, blockchain technology is made of a chain of blocks that can transact with each other even though they do not trust themselves. Also, blockchain addresses the problems related to certificate generation and verification by providing verifiable tools consisting of records marked with a timestamp that is immune to modification (Dawi, Jusoh, Streimikis & Mardani, 2018). To this end, studies have identified blockchain technology as possessing the potential to deal with the matter of authenticating certificates

adequately. Hence, this study aims to develop a certificate generation and verification system that employs the use of blockchain technology and Quick response (QR) code in providing security, anonymous, simple and easy to use platforms for institutions, organizations or anyone concerned to verify the authenticity of educational certificates.

1.1 STATEMENT OF PROBLEM

Issued certificates are designed to be authentic when verified. However, over the years there are many cases of certificate forgery in most organizations and even educational institutions (Saleh, Ghazali & Rana, 2020). Furthermore, differentiating fake and original certificates needs a lot of concentration and end in the wastage of valuable time (Ravi, Devdoot, Hitesh & Bharati, 2021). Such cases arouse the need for fast and easier means of certificate verification to minimize the level of certificates forgery. In the light of this development, different kinds of verification systems were developed to curtail this problem. But these systems mostly adapt the use of Relational Database Management System (RDMS) which is now easily hacked with the advancement in technology (Nwachukwu & Igbajar, 2015). Also, the security features are mostly single mode, which is the use of login IDs and passwords only (Kumar & Senthil, 2019). Thus, making these application systems vulnerable and inefficient for such a huge task.

Hence, this study develops and implement a Certificate Generation and Verification System (CVS) that will adopt the use of blockchain technology and Quick Response (QR) code to mitigate the above-stated problems. Blockchain offers a certifiable distributed archive using a cryptography mechanism to counter forged official certificates (Ravi et al., 2021). The Blockchain also provides a shared platform for storage, retrieving the document and decreasing the overall verification time.

II. Literature Survey

Several efforts have been made by researchers to verify and authenticate certificates to eradicate the issue of certificate forgery. Nonetheless, the certificate verification method is still prevalent today as a result of the existence of a manual process, whereby individuals or organizations interested in verifying a certificate trips to the institution or send a written request.

Given the above, Musee (2015) in his work adopted the use of the Agile Methodology approach vis-à-vis Unified Process modelling to develop a cloud-based prototype that is used to provide certificate verification. This prototype permitted users to request and generate their academic credentials authenticated by supplying information such as the name of the institution, the course title, graduation year and the verification token. All these procedures were carried out in a private cloud and it is available online. However, the key shortcoming of the system is the use of the Relational Database Management System (RDBMS) which does not support horizontal scaling that is partitioning or sharing.

Osman and Umar (2016) combined a cloud-based model and cryptographic method to improve the authentication of certificates and thereby decrease the rate of certificate counterfeit predominance. The essence is to develop a model that will ensure confidentiality, validity and security of educational certificates is enhanced. By using the Cloud-based model, a number of the factors that end in reduced operational efficiency in student services at universities are often addressed and this could have a positive impact on the standard of services provided by universities. However, the cost of implementing this model is high since the cloud infrastructures are owned and managed by a third party known as service providers. Thus, most institutions could not afford its implementation due to the fact it's expensive to be adopted.

Zheng et al. (2017) in their work introduced different terms about blockchain technology and the most vital concept termed smart contract. In their work, the data hash to be kept in its previous block forms a long chain of nodes. The hash changes, if there is any change in the data and won't match with the hash value stored in the previous block and hence letting us know about the tampering of data. Once tempered data is noticed in a block, the hash of the block changes and it remain unrecognized in the chain. Unfortunately, their work needs to be implemented to fully understand and framework

Singhal and Pavithr (2018) combined a Quick Response (QR) code and smartphone application to develop a certificate verification system. The quick response code comprises an electronic signature over information such as student's name, matriculation number, graduation year; class of degree etc. which will be signed up by the institution designated authorities. Verifying the digital signature appended on each certificate, anybody interested will have to use a particular application to scan the QR Code and validate the certificate. However, the system stores the record of each QR code appended on the generated certificates which is insecure and unreliable.

Yusuf et al. (2018) in their research work "Automated Batch Certificate Generation and Verification System" allowed an end-user to define the format and template of a certificate with little or no requisite of XML knowledge via clicking buttons and keying from the system Graphical User Interface (GUI), verifying the certificate and generating one or more certificate(s) concurrently. In this system, students' records are keyed and

imported into the system via an excel file, consequently, making the system partially automated and inefficient for verifying certificates.

Jiin-Chiou et al. (2018) in their research, proposed a blockchain certificate verification system with a design consisting of three (3) actors. These actors were institutions, the students, and lastly the service provider. The deficiency of their method was that they used one hash as a key which makes it publicly accessible once the hash key is known.

Neehu & Vani (2018) developed a web certificate verification system where organizations, institutions or anyone concerned would be able to verify the authenticity of certificates presented to them. However, this system employs the use of Login IDs and Passwords alone which is a single mode of system security making it accessible to anyone that knows the login credentials, as such security.

San et al. (2019) developed a certificate verification system implementing trusted ledgers of blockchain. In this system, end users have full control of their data thanks to wallets and private keys. But the system requires average users to have an in-depth knowledge of blockchain technology. Also, the system was developed and implemented in a public blockchain. However, this system is not secured and reliable due to the lack of a mechanism to preserve data privacy.

Obilikwu, Usman and Kwaghtyo (2019) adopted a top-down design approach and iterative model to develop a generic certificate verification system for Nigerian universities. The process of certificate verification in this system supports horizontal scaling or sharding as the system was implemented using the Mongo database. Also, the system was able to solve the problems associated with certificates verification with the provision of a centralized database storing the records of certificates generated through the use of certificate numbers. Unfortunately, the system consumes high memory of data and lacks flexibility since it can only be implemented in some selected schools.

Gaonkar et al. (2020) implemented a certificate issuing system centred on an online sign-up system to ease the burden to the institutional administrators. Using certificate-based authentication instead of ID/password-based one is considered effective in improving both the usability and the stability of eduroam. But this system lacks integrity as certificates can be forged and replicated. Also, a centralized database used to house such data is not secured as it can be hacked with recent technological advancements.

Saleh et al. (2020) in their work titled “Blockchain-Based Framework for Educational Certificates Verification” proposed a blockchain-based framework for educational certificate verification focusing on specific themes based on the hyper ledger. The security themes required for educational certificates verification in the blockchain are authorization, authentication, confidentiality, ownership and privacy. But the proposed framework lacks flexibility since it can only be implemented and adopted in some selected educational institutions.

Aniket, Sagar and Shivraj (2020) suggested that a digital certificate system is required to curtail the problem of certificate forgery. In their work, they proposed a blockchain-based certificate verification system that validates the authenticity of academic certificates through the use of digital signatures and timestamps. However, this adoption will be very expensive to implement and the said digital signature can be forged due to advancements in technology which makes the system less secured and unreliable.

III. Methodology

This paper adopts the use of Iterative and Incremental development models of the software development life cycle. The incremental model involves breaking down the software development processes into trivial and manageable pieces known as increments. Every single increment builds on the preceding version so that progress is made in a step stepwise approach. Whereas the Iterative model encompasses software developmental processes being analytically repeated in cycles known as iterations. A different version of the software is produced after each iteration until the optimal product is achieved. With these two approaches, improvements are made on an ongoing basis likewise changes can be made in the process rather than waiting until the end of the software development. These models will be used since the requirements of the complete system will be clearly defined and understood, and they also support functionalities or requested enhancements that may evolve with time. The diagram is shown in Figure 3.1.

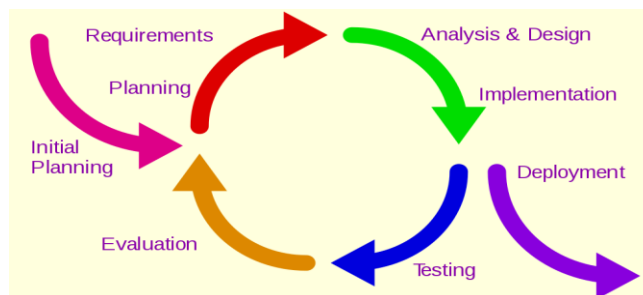


Figure 3. 1: Iterative and Incremental model Ehtesham et al, (2018)

3.1 Proposed System Framework

In this subsection, the framework of the new system is presented in Figure 3.2 indicates what a student, verifier, and university can do. To create certificates on the blockchain-based system, firstly, the university will have to be registered. Once added the university will have access to the system to generate certificates either in bulk using a predefined CSV template or a singly one with the aid of data fields control. Each certificate generated will be kept in the format of an Interplanetary File System (IPFS), and the unique hash ID and QR code will automatically be generated using the SHA-256 algorithm. The generated hash ID and certificates details will be kept in the blockchain network and registered students will receive their hash IDs and QR codes respectively.

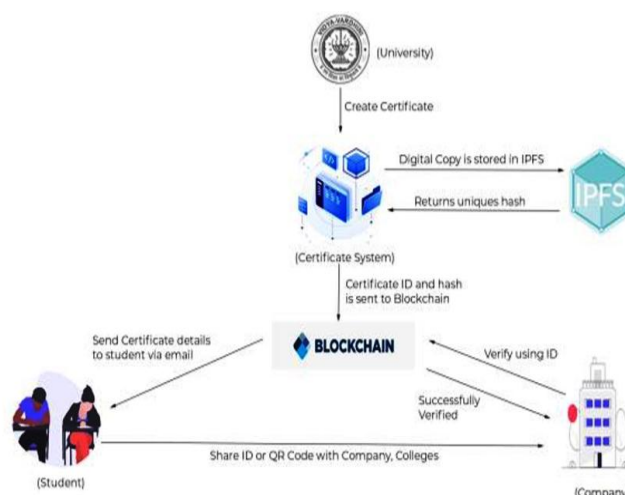


Figure 3. 2: New System Framework Ravi et al, (2021)

The verifier or anyone can validate the authenticity of any certificate using the hash or QR code and can as well compare the submitted copy with the one displayed by the system. Additionally, the certificate is immune to any alterations or modifications that may be subsequently requested by an intruder.

3.2 Architecture of the New System

In this subsection, the architectural design of the newly developed system is presented in Figure 3.3. The diagram is made of four components. They include clients, IPFS (Interplanetary File System), Database and Blockchain. The client could be the user, admin or institutes verifying the certificates. The client sends a request to the system which is the whole server, and before the request gets processed, it has to pass through the spring security and JWT (JSON Web Token) to authenticate the user and validate the incoming request. After the request has successfully passed through the security layer, then it goes to the request processor where the request is processed by services and controllers and the response is returned and sent back to the client. The IPFS (Interplanetary File System) is used for storage purposes and processes. In this architectural diagram, the IPFS stores certificate documents and information. While the database stores data and information of the system entities. Information residing in the database include user details and certificates information. The system also communicates with the blockchain network to generate hash code for each certificate and the same communication link is maintained when verifying the certificates or strolls.

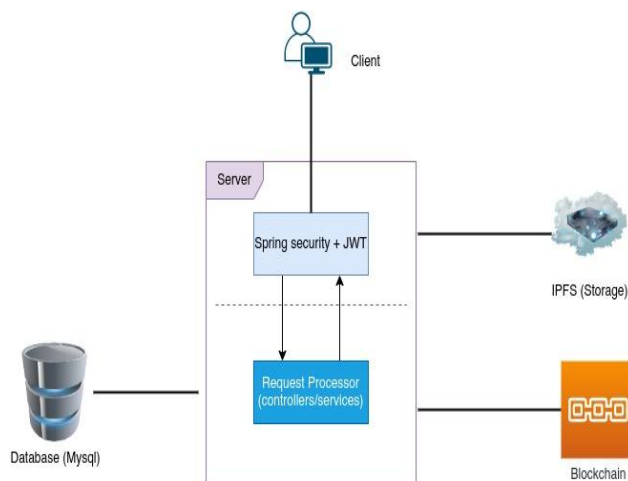


Figure 3. 3: Architectural Diagram of the New System

As seen in Figure 3.1, all these processes are being carried out after successfully passing through the security layer. Though, it is not all requests that require authentication such as verifying certificates. When verifying certificates, the user does not have to log in and hence there is no need for authentication. However, administrative requests that have to do with adding and modifying data needs authentication.

The spring security manages sessions and information of users currently login while the JWT is responsible for sending authentication tokens. What happens is that when a user logs in, a token will be created for the user and for every request that the user makes the token will be passed to verify whether it is a valid user and the user has a login or not. Accordingly, the JWT will, first of all, take the request, validate the user and confirm if the token is expired or not. Even if the token is valid or expired, the JWT will notify the spring security since the decision to execute or decline the request processing is the sole responsibility of the spring security. Additionally, if the JWT successfully verify the user, and the user has login and has a valid token then the spring security send the request to the request processor for processing and the response will be returned and sent to the user. On the contrary, if the user verification fails then the spring security forbid the execution of the request. The server is having the security layer and the request processor layer.

3.3 Algorithm and Flowchart of the System

Algorithm of the system

1. Begin
2. Upload student records
3. If records already exist
Go to step 8
Else
Print "Upload successful"
4. Create certificates
5. Store certificates in IPFS
6. Generate certificate with hash_code
7. Generate QR code
8. Preview Certificate
9. Send certificate_details to student via

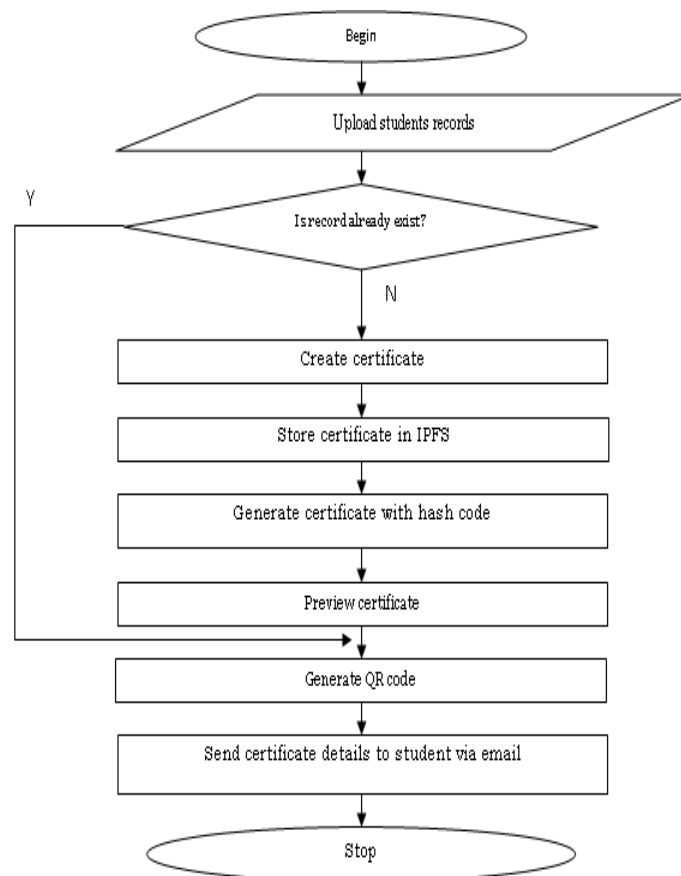


Figure 3. 4: Flowchart of the System

IV. Results And Discussions

This section shows the result of the implemented certificate generation and verification system and the performance is also considered.

4.1.1 Certificate Generation Process

The university which serves as the certificate issuer in this system has two options provided to generate certificates. The first option is to fill in details in a form to generate a single certificate as shown in figure 4.1 while the second option involves uploading Comma-Separated Values (CSV) to make certificates in bulk as shown in figure 4.2.



Figure 4. 1: Form to Generate Certificates

The Certificate issuer will first be asked to feed in their certificate template. Depending upon the number of fields the issuer will be asked to fill in the data of the respective fields. The system will grab that data and append it to the pre-inserted template.

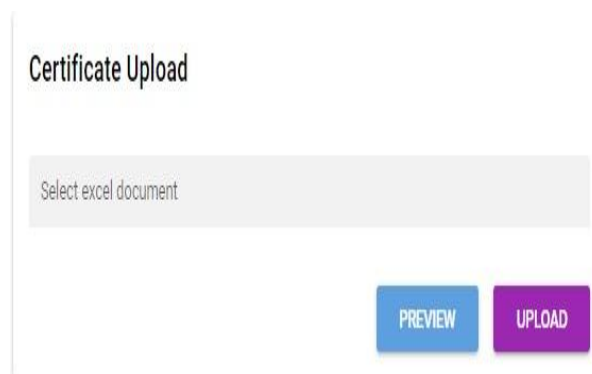


Figure 4. 2: Form to Generate Multiple Certificates

A preview will be generated for the certificate as shown in figure 4.3. If the issuer uploads it then the system runs its hashing algorithm and store it. The same hash will be forwarded to Blockchain Node and it will be saved in the Blockchain.

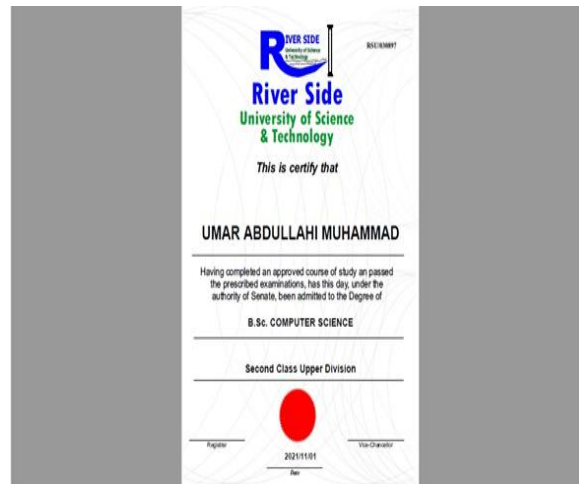


Figure 4. 3: Preview of Generated Certificate

After successfully generating the certificate, the certificate ID and a QR Code will be sent to the registered email address to view a certificate as shown in figure 4.4



Figure 4. 4: Mail sent to Student

4.1.2 Certificate Verification process

The Validator is the company or organization's authority who will need to validate the originality of certificates of graduates or students applying for a job or seeking admission. The verifier has two options in this system- verify entering student hash ID or verifying using QR code supplied by the student or graduate.

Verification Using Hash ID

The validator type in the unique ID for the certificate to be authenticated as shown in figure 4.5. A preview of the certificate is generated if the typed hash ID matches the ID stored in the blockchain as depicted in figure 4.6. Otherwise, an error message is returned indicating verification failed as shown in figure 4.7.

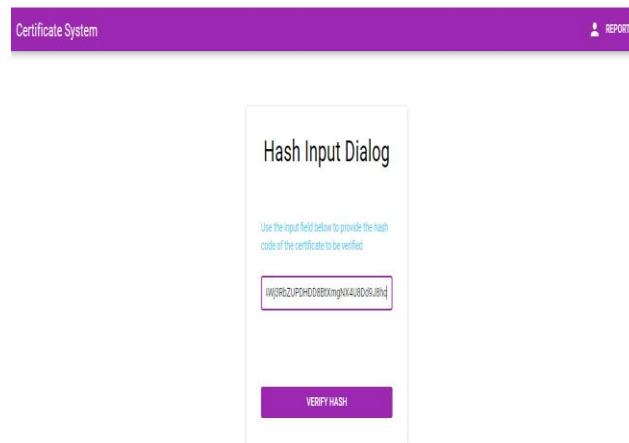


Figure 4. 5: Hash ID input being given for verification



Figure 4. 6: Successful Verification of Document generates preview and prints the data

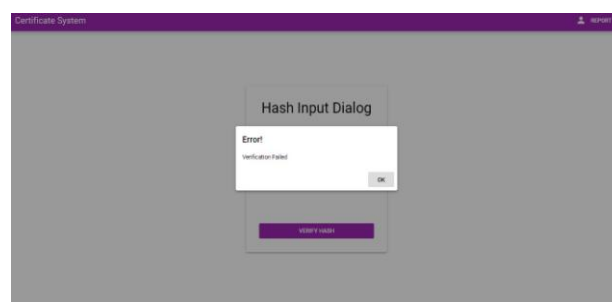


Figure 4. 7: An invalid Certificate ID being rejected

Verification Using QR Code

Another option for the validator is to directly scan the QR code-shared (as shown in figure 4.8) by students or graduates at the point of application or entry. This verification process can be achieved through the use of QR Code Extension found in chrome, firefox and internet explorer. Similarly, this process can also be achieved on mobile devices with the aid of applications such as QR code scanners.



Figure 4. 8: QR code-shared by students or graduates

If the scanned QR code matches the one in the system, then a preview of the certificate is presented as shown in figure 4.6. While on the contrary, if the scanned QR code does not match the one in the system, then an error message is returned indicating verification failed as shown in figure 4.7.

V. Conclusion

This paper studied how certificates generation and verification is being carried out and develop a certificate verification system based on blockchain technology and quick response code that aims to provide improvements to the various weaknesses that are associated with the existing system. The system was implemented in a way that only the university (Administrator) can create and upload certificates in the blockchain system, and once these certificates are created no alterations can be made. This feature helps us to achieve a system in which all the process is transparent and unchangeable. Our System automates the process of generating certificates and reduces the manual work needed for the verification of the same. Students are also at comparatively low risk of losing the certificate. By adding QR code as an additional feature, the system decreases the percentage of data being tampered with and possibly make it difficult and unreliable. The Hash of the certificate is being stored in the blockchain while the original document will be stored in the Interplanetary File System (IPFS). This will help us preserve the data and create transparency.

5.1 FUTURE WORK

Some of the recommended areas that can be visited for further research are:

- i. Further work can include an access control system for the admin application to make sure that not just anybody can visit the admin page but just the university authority.
- ii. The server can make use of sessions to make sure that people can only interact with the system through the client application.
- iii. Fingerprint and facial recognition systems may be added to enforce security and flexibility.

Reference

- [1]. Aniket, V. R., Sagar, S. J., Shivraj, M. P. & Madhavi G. P. (2020). Education Degree Fraud Detection and Student Certificate Verification Using Blockchain. *International Journal of Scientific Research and Engineering Development*, 3 (1), 287-289.
- [2]. Dawi, N. M., Jusoh, A., Streimikis, J., & Mardani, A. (2018). The influence of service quality on customer satisfaction and customer behavioural intentions by moderating role of switching barriers in satellite pay TV market. *Economics and Sociology*, 11(4), 198-218. doi:10.14254/2071-789X.2018/11-4/13
- [3]. Ehtesham Chowdhury, A. Z. M., Bhowmik, A., Hasan, H., & Shamsur Rahim, M. (2018). Analysis of the Veracities of Industry Used Software Development Life Cycle Methodologies. *arXiv e-prints*, arXiv-1805.
- [4]. Gaonkar, P., Daruwale, P., & Nagmani, K. (2020). Centralized Digital Certificate Issuing System.
- [5]. Javier, R. S., Javier H., Oscar, M., & Manel, M. (2004). Securing Certificate Revocation through Speaker Verification: the CertiVeR Project. 2nd COST 275 Workshop - Biometrics on the Internet.
- [6]. Jiin-Chiou, Narn-Yih, L., Chien C., & YI-Hua, C. (2018). "Blockchain and Smart Contract for Digital Certificate," *Proceedings of IEEE international Conference on Applied System Innovation*.
- [7]. Musee, M.N. (2015). An academic certification verification system based on a cloud computing environment. 55-88.
- [8]. Neehu, G. & Vani, V. P. (2018). Survey on Blockchain-Based Digital Certificate System. *International Research Journal for Engineering and Technology*, 5(11), 1244-1248.
- [9]. Nwachukwu, K.C., & Igbajar, A. (2015). Designing an Automatic Web-Based Certificate Verification System for Institutions. *Journal of Multidisciplinary Engineering Science and Technology*, 2(12), 3159-0040.
- [10]. Obilikwu, P., Usman, K., & Kwaghtyo, K. D. (2019). A Generic Certificate Verification System for Nigerian Universities.
- [11]. Osman, G., and Omar, S.S. (2016). Cloud-Based Graduation Certificate Verification Model. *Proceedings of Academics World 54th International Conference*, Malacca, Malaysia. Retrieved from https://www.worldresearchlibrary.org/up_proc/pdf/57114861269431620.pdf
- [12]. Patrick O., Karim U., & Kenneth D. K. (2019). Generic Certificate Verification System for Nigerian Universities. *International Journal of Computer Science and Mobile Computing*, 8(10), 137-148.
- [13]. Ravi, S. L., Devdoot, M., Hitesh, S., & Bharati, G. (2021). Certificate Verification using Blockchain and Generation of Transcript. *International Journal of Engineering Research & Technology (IJERT)*, Vol. 10 Issue 03, 2278-0181.

- [14]. Saleh, O. S., Ghazali, O., & Rana, M. E. (2020). Blockchain-based framework for educational certificates verification. *Studies, Planning and Follow-up Directorate. Ministry of Higher Education and Scientific Research, Baghdad, Iraq. School.*
- [15]. San, A. M., Chotikakamthorn, N., & Sathitwiriawong, C. (2019). Blockchain-Based Learning Credential Verification System with Recipient Privacy Control. In *2019 IEEE International Conference on Engineering, Technology and Education (TALE)* (pp. 1-5). IEEE.
- [16]. Senthil, M., & Kumar, P. (2019). Tamper-proof birth certificate using blockchain technology. *International Journal of Recent Technology and Engineering (IJRTE)*, 7(5S3), 95-98.
- [17]. Singhal, A., and Pavithr. R.S. (2018). Degree Certificate Authentication using QR Code and Smartphone. *International Journal of Computer Applications*, 120(16), 0975–8887. Retrieved from <https://docshare01.docshare.tips/files/29369/293691731.pdf>
- [18]. Xu, Y., Chong, H. Y., & Chi, M. (2021). A Review of Smart Contracts Applications in Various Industries: A Procurement Perspective. *Advances in Civil Engineering*, 2021.
- [19]. Yusuf, D.A., Boukar, M.M., and Shamiluulu, S. (2018). Automated Batch Certificate Generation and Verification System. Conference Paper. Retrieved from https://www.researchgate.net/publication/324531116_ICECCO
- [20]. Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017). An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends,” *Proc. - 2017 IEEE 6th Int. Congr. Big Data, BigData Congr.*, no. June, pp. 557.

Muhammad Umar Abdullahi, et. al. “Certificate Generation and Verification System Using Blockchain Technology and Quick Response Code.” *IOSR Journal of Computer Engineering (IOSR-JCE)*, 24(1), 2022, pp. 37-47.