Scientific Research Publishing

Journal of Computer and Communications, 2023, 11, 73-82
https://www.scirp.org/journal/jcc
ISSN Online: 2327-5227
ISSN Print: 2327-5219

Blockchain-Based Certificate Authentication System with Enabling Correction

Md. Mijanur Rahman, Md. Tanzinul Kabir Tonmoy, Saifur Rahman Shihab, Riya Farhana

Department of Computer Science and Engineering, Southeast University, Dhaka, Bangladesh
Email: mijanur.rahman@seu.edu.bd, tanzinulkabir@gmail.com, rahmansaifur223@gmail.com, riyafarhana56@gmail.com

How to cite this paper: Rahman, Md.M., Tonmoy, Md.T.K., Shihab, S.R. and Farhana, R. (2023) Blockchain-Based Certificate Authentication System with Enabling Correction. *Journal of Computer and Communications*, **11**, 73-82.
https://doi.org/10.4236/jcc.2023.113006

Received: February 3, 2023
Accepted: March 28, 2023
Published: March 31, 2023

Abstract

Blockchain has proven to be an emerging technology in the digital world, changing the way everyone thinks about data security and bringing efficiency to several industries. It has already been applied to a wide range of applications, from financial services and supply chain management to voting systems and identity verification. An organization must verify its candidates before selecting them. Choosing an unqualified candidate can ruin an organization's reputation. In this paper, a blockchain-based academic certificate authentication system will be used to ensure authenticity and make the assertion of the decentralized system secure. However, the system will generate, authenticate and make corrections on academic certificates. Ultimately, some blockchain-based authentication systems already exist, they can't correct any errors that occur during generation. A blockchain-based certificate authentication system was built using blockchain technology. Where admin could generate, authenticate and correct the certificate if necessary. The admin can also check how many times a certificate has been modified. Other users can only check the authenticity of the certificates. We're using two blockchains to enable corrections. Blockchain technology can successfully implement a certificate authentication system. This system will eliminate doubts about the authenticity of certificates, provide fast responses, and ensure reliable and secure storage. The proposed system will help in many ways, such as providing a user-friendly university admission, and smooth job hiring process, etc. In conclusion, our proposed system can permanently eradicate certificate forgeries and create and promote trust in society.

Keywords

Blockchain, Certificate Authentication, Certificate Correction, Secure Certification, Eliminate Forging

1. Introduction

In our daily lives, certificates play an invaluable role [1]. It is a document that is provided to a student when he/she graduates from a school, college or university. Human capital is defined as the knowledge, skills, and abilities gained via education [2]. A student's credentials serve as a testament to his or her diligent work over the years. Those graduate students need these certificates to apply for higher education or to obtain employment in respectable places. In both circumstances, they need to provide their credentials for validation. To validate, institutes check the authenticity of certificates provided by candidates. After validation, candidates proceed to the next stage. To validate the authenticity of a certificate, the institute uses a third-party system or direct contacts with the institute from which it was generated which is often a time-consuming and complicated process.

The United States currently has 2 million fake degree certificates and 300 unauthorized universities [3]. If proper validation was not conducted, then any unworthy candidates who had resorted to forgery of their qualifications would be hired. The reason behind certificate forgery is that many unethical people want to get their dream job without having the necessary qualifications, so they provide fake certificates in order to deceive the hiring company. This makes the validation process much more difficult and time-consuming, as the hiring company must now carefully scrutinize the qualifications of each candidate to ensure their legitimacy. A study shows that almost 10% of applications given by candidates are forged [4]. Applicants tend to lie about their education and experience [5]. Every year, academic certificate fraud costs employers approximately $600 billion [6].

"The phenomenon of fake academic degrees is a threat to any community. It is an enormous threat, both for the present and the future" [7]. Nowadays there are numerous cases of certificate forging in the news. In recent years, certificate forgeries have increased due to advances in scanning and printing technologies. As a result, the integrity of both the certificate holder and the institute that issued the certificate is at risk [8]. For 28 years, the Massachusetts Institute of Technology's dean of admissions was found to have faked and misled the institute about her academic qualifications [9].

Certificate forging is also causing problems in the medical field. Many people pretend to be a doctor by forging fake certificates. As a result, people from all socioeconomic backgrounds will not receive equal treatment when they visit different types of doctors [10]. A similar report was published in Bangladesh. It was for using expired reagents and selling unapproved drugs. Seven employees, including two fake doctors, were sentenced to indeterminate jail terms and penalties for taking high charges from patients and providing fake medical reports [11]. In Mexico, there are some aesthetic pseudo-clinics with non-medical personnel performing surgery on patients which caused many complications [12].

Blockchain is one of the most popular technologies that transform the way we live at the moment. Blockchain is a decentralized database that contains records called a block. Each block contains its timestamp, hash or address of the previous block and the data of the block. Each block has a unique hash that can be used to track back to its previous block. A hash is a function that converts a set of data into a fixed-size data structure, called a hash value. Blockchain technology has several applications, including cryptocurrency, smart contracts, supply chain management, and more. Stuart Haber and W. Scott Stornetta, two mathematicians who wanted to implement a system where document timestamps could not be tampered with, proposed blockchain technology in 1991 [13]. Since the information on the blockchain is unchangeable, it gives assurance that no one can tamper with the information. If any attempt is made, it can easily be identified because of the changes in the hash value [13]. As the authors point out [14], traditional authentication methods do not provide security, tamper-proofing, or authentication for documents. For this reason, blockchain is best suited to our system.

Based on this study, we proposed a system to resolve a crucial pair of problems in the world of education and job hiring using blockchain technology. The system will verify whether the certificates are given by any legitimate organization or academy. The system will permanently store all the credentials securely, making the authentication process much easier and more convenient, and eliminating the crime of certificate forging. The system will also have correction functionality so that if any modifications need to be done, the authority can easily accomplish them.

2. Literature Review

Blockchain was introduced long before Bitcoin was introduced by Satoshi Nakamoto [15] [16]. However, blockchain gained its popularity with Bitcoin. Although bitcoin is sometimes referred to as a blockchain by some people, but the fact is bitcoin was built using blockchain technology. In a short period of time, blockchain became popular when people discovered its salient benefits. It has become one of the top technologies worldwide. For this reason, many studies and research were conducted and this proposed system rewired some of them.

Authors of [17] have made some excellent points about blockchain architecture and consensus algorithms. They have also examined the limitations of blockchain and given some possible solutions. They also investigate various consensus algorithms in different respects and discuss their differences. By analyzing those differences, they can determine the most appropriate consensus algorithm.

The author of [4] Rishabh Garg, has examined how blockchain technology can be applied to solve problems within academic institutes and the employment sector. According to the author, blockchain will be the panacea for this issue. He proposed a framework that can issue new certificates as well as validate them.

In Osman Ghazali and Omar S. Sale [18], emphasized the significance of certificate verification and its influence in our society. In the paper, traditional verification processes were briefly explained, as well as their limitations. To eliminate those limitations, they proposed a blockchain-based verification system. A system that is not only used for verification but also for generating new certificates. They will generate digitally signed certificates using the asymmetric key and timestamp. Students will receive a copy, which they can verify in the system.

Jayesh G. Dongre and his colleagues proposed [19] to solve the problems of the current system of certificate verification. In the paper, they talked about the current verification process and the proliferation of certificate fraud. Using blockchain, they have developed a platform for validating and generating certificates. In their view, the use of blockchain for certificate verification is beneficial to society. It will eliminate certificate fraud.

R. Suganthalakshmi [20] and her colleagues investigated an optimal method of verifying academic credentials in 2022. The number of graduating students is increasing every year, and it is becoming increasingly necessary to validate their academic credentials. Without proper validation, any ineligible candidate will be blessed with opportunities. Their solution is to create a platform for all certificates a student may possess. Students upload all their credentials to the system, and the system stores them on the blockchain. To verify a credential, a person needs the student's ID and password. They used the PoW (Proof of work) consensus algorithm for validation, but the validation method was not well elucidated.

In the papers mentioned, researchers are interested in building a system to verify and generate academic credentials. Although their system design is different from each other but they all agree on using blockchain for security. Our proposed system can also generate and verify academic credentials, as well as modify them. There is a possibility of making a mistake when generating certificates. Our study found that none of the papers offered editing options if any modifications were needed. We provide an editing facility option to fix those errors.

3. Methodology

In this study, the general idea of the proposed system is depicted in **Figure 1**. There will be two actors, the university (Admin), and other users (Students/Employer). The university is authorized to generate new certificates for students, make corrections if necessary, and authenticate the certificates. On the other hand, general users are allowed only to confirm the authenticity or view the certificates. The user in this category can't make any corrections or generate new certificates. We utilize two chains in our system. One is for storing certificate data and the other is for keeping track of corrections.

The certificate generation process is shown in **Figure 2**. In this system, everyone can check the authenticity of the certificates but not everyone can generate or add new certificates to the system. Only authorized persons will be allowed. First, an authorized person needs to prove their identity by login in. After proving

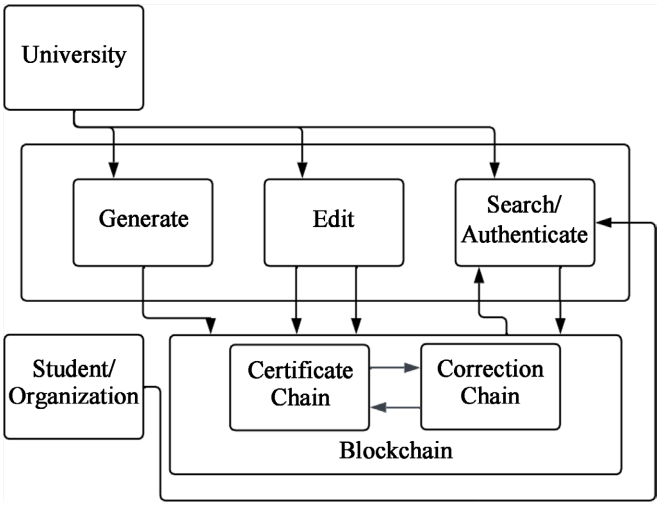

Figure 1. System architecture.

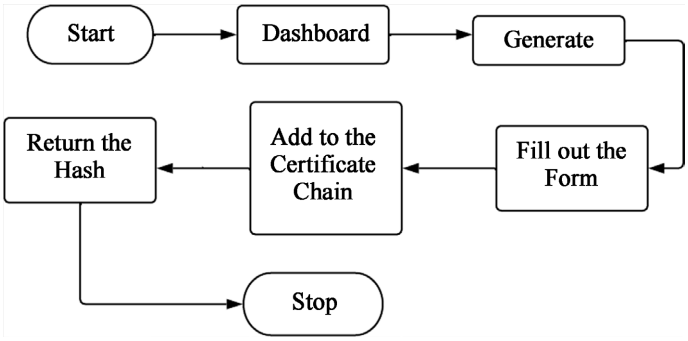

Figure 2. Generating new certificates.

their identity, they can add a new certificate to the blockchain. To add a certificate, the user may need to fill up a form. In that form, they have to provide the information of the candidate. After hitting submission, the system will generate a new block and store the data on the certificate chain. After that, it will return the block address to the university and the student.

PSEUDOCODE 1: Function to generate Certificate

```
function generate Certificate(Arguments) public {
check if authorized to generate a Certificate
then store the certificate
return the address of the certificate
}
```

The certificate correction process is depicted in **Figure 3**. To correct a certificate, we need to provide the system with the address of the old block and the updated data. After getting those two pieces of information our system will generate two new blocks. The first block will contain corrected data and it will be stored in the certificate chain. The second block will contain the hash address of the old certificate and the hash address of the corrected block. However, the modified block will be stored in the correction chain as a reference point.

PSEUDOCODE 2: Function to make correction
function correct Certificate (Argument old_Certificate_addressother arguments) public {Check if authorized to perform the correction. Then check if old_Certificate_address exists on the certificate chain.
Store new certificate on certificate chain.
Store old and new certificate addresses on the correction chain.
return the corrected certificate address.
}

The validation-checking process is shown in Figure 4. In our system, a certificate can be checked in two ways. This can either be done by manual typing or

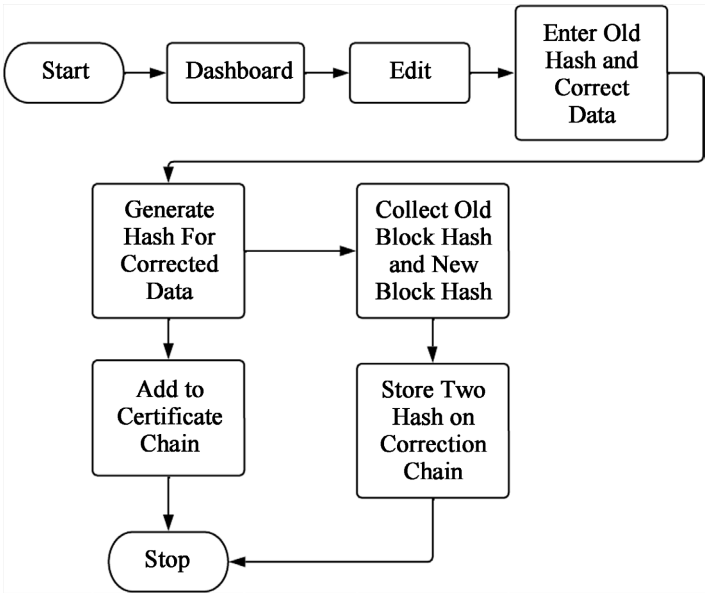

Figure 3. Certificate correction.

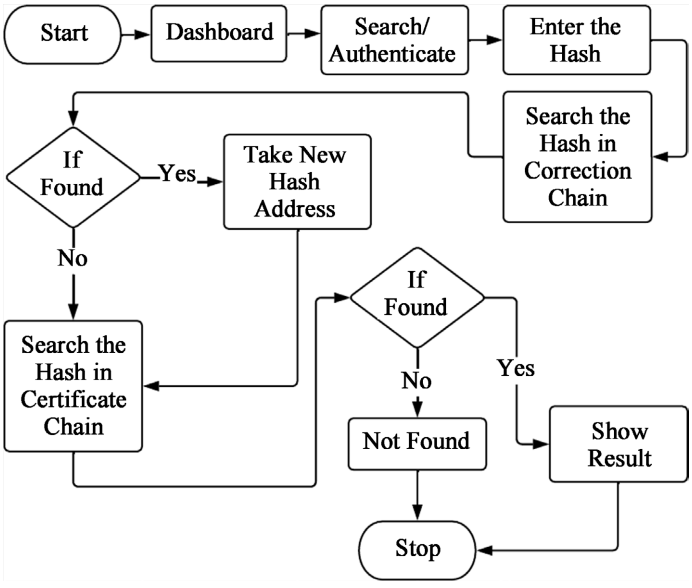

Figure 4. Checking the authenticity.

scanning the QR code. QR code will contain the hash address of the block where the data is stored. Apparently, the system will look for the hash address in the correction chain. Upon finding a match, the system will get the corresponding new certificate hash from the block. Later, it will search for the hash in the certificate chain and display the result. When the system is not able to locate the hash address in the correction chain, it searches the certificate chain and displays the result. If the system could not locate the hash address in both chains, then it will show certificate does not exist.

PSEUDOCODE 3: Function to Authenticate
function authenticate (Argument address) public {
check if exists on the correction chain then get a
new certificate address and check if a new certificate address exists on the certificate chain then return the corrected certificate.
else return "Not Exist"
else check if exists on the certificate chain
then return the certificate else return "Certificate does not exist"
}

4. Result and Discussion

In our proposed system, we adopted Remix IDE for writing and developing our smart contract. For testing, we deployed the smart contract on Remix's virtual network. Our study estimated three primary functions: 1) Generate Certificate, 2) Correct Certificate and 3) Authenticate Certificate. Upon deploying the smart contract in the Remix virtual machine, it gives us information about the transaction hash, gas fee, and more which is illustrated in Figure 5.

After successfully testing the smart contract on Remix's virtual network, we deploy the code on the Goerlitestnet network, which is illustrated in Figure 6. During the deployment phase, it asks for confirmation. Our metamask wallet confirms it. After successfully deploying the smart contract on the blockchain, we obtained the address and the ABI (Application Binary Interface) of the smart contract from Remix IDE and the medium of our front-end connection with the blockchain.

Figure 5. Deploy on Remix IDE.

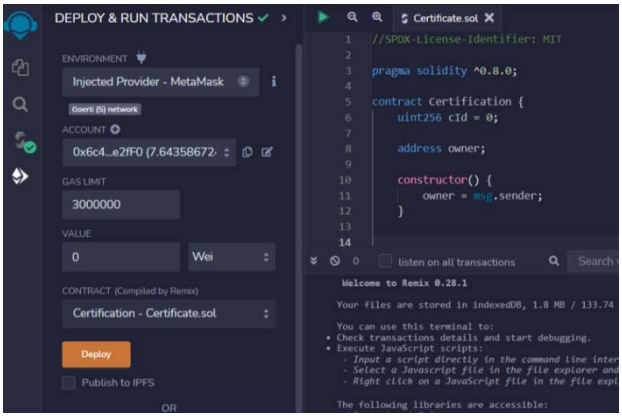

Figure 6. Deploy to Goerlitestnet.

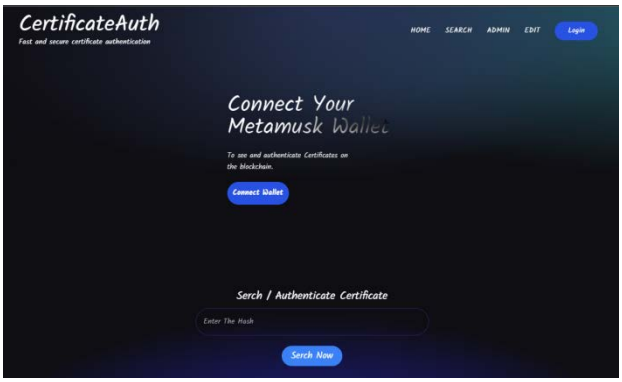

Figure 7. Web Application.

Figure 7 shows the frontend web application of the proposed system.

Our testing showed that the system could successfully generate and authenticate certificates on the blockchain. We were also able to correct errors in the certificate, which is a unique feature that is not available in existing blockchain-based certificate authentication systems. The development of a blockchain-based academic certificate authentication system has the potential to revolutionize the way academic certificates are verified and authenticated. By using blockchain technology, we can ensure the authenticity of certificates and prevent forgery, which can have a significant impact on the reputation of organizations that rely on certificates for selecting candidates. Overall, our proposed system has the potential to permanently eradicate certificate forgeries and create and promote trust in society, leading to a user-friendly university admission process, and a smooth job hiring process, among other benefits.

5. Conclusions

Because many candidates fabricate certificates, traditional validation methods are facing new challenges in the digital age. Fabrication of certificates occurs in order to gain admission to prestigious universities or to obtain a satisfactory job. To overcome those challenges, the validation process needs to be more advanced and secure. Blockchain technology is ideal for tackling those challenges. Due to

the enormous characteristics of blockchain, such as decentralization, census, and security, it has become one of the leading technologies in recent years. Our proposed system is built on a blockchain architecture. It will not only validate certificates but also has the ability to generate brand-new certificates for students. Other blockchain-based verification platforms only offer verification and the ability to generate new certificates, but don't allow the correction of certificates. However, during the process of creating the certificate, a mistake can occur. If there is no way to make up for those mistakes, then it is not an ideal platform. In this proposed system if any mistakes were made, they can be fixed and by eliminating certificate forgeries and creating a trustworthy environment, the system will guarantee the integrity of certificates.

As the system develops, it can be expanded to include blockchain-based professional degree management, implementation of an NID (National Identity Card) verification system, and other blockchain-based systems.

Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

References

[1] Healy, T., Cote, S., Helliwell, J. and Field, S. (2001) The Well-Being of Nations: The Role of Human and Social Capital. OECD, 118.

[2] Baum, S., Ma, J. and Payea, K. (2013) Education Pays 2013. The College Board, New York, 1-48.

[3] Grolleau, G., Lakhal, T. and Mzoughi, N. (2008) An Introduction to the Economics of Fake Degrees. *Journal of Economic*, **42**, 673-693. https://doi.org/10.1080/00213624.2008.11507173

[4] Garg, R. (2021) Blockchain Ecosystem for Education & Employment Verification. *Proceedings of* 13*th International Conference on Network & Communication Security* (*NCS* 2021), Toronto, 25-26 September 2021.

[5] Share, E., Memorable, M. and They, L. (2014) Fifty-Eight Percent of Employers Have Caught a Lie on a Resume.

[6] Garwe, E.C. (2015) Qualification, Award and Recognition Fraud in Higher Education in Zimbabwe. *Journal of Studies in Education*, **5**, 119-135. https://doi.org/10.5296/jse.v5i2.7456

[7] Al Suwaidi, J.S. (2019) Fake Academic Degrees: A Crime against the Present and the Future. https://gulfnews.com/opinion/op-eds/fake-academic-degrees-a-crime-against-the-present-and-the-future-1.66162272

[8] Sheng, C.A.O., Chen, Z. and Sun, X. (2017) Anti-Counterfeit Authentication System of Printed Information Based on a Logic Signing Technique. *Proceedings of the* 2007 *International Conference on Intelligent Systems and Knowledge Engineering* (*ISKE* 2007), Chengdu, 15-16 October 2007, 1254-1259.

[9] Lewin, T. (2007) Dean at M.I.T. Resigns, Ending a 28-Year Lie. https://www.nytimes.com/2007/04/27/us/27mit.html

[10] Ahmed, T. (2021) The Case of Doctor-Patient Relationship in Bangladesh: An Application of Relational Model of Autonomy. *Bangladesh Journal of Bioethics*, **12**, 14-24. https://doi.org/10.3329/bioethics.v12i1.51900

[11] Mohiuddin, A. (2019) An A-Z Pharmaceutical Industry: Bangladesh Perspective. *Asian Journal of Research in Pharmaceutical Science*, **9**, 17-28. https://doi.org/10.5958/2231-5659.2019.00004.3

[12] Tristán, F.A.P. *et al.* (2021) Foreign Modeling Agent Reaction; Managed with Two Staged Surgical Reconstruction. Case Report and Review of Literature. *International Journal of Surgery Case Reports*, **84**, Article ID: 106137. https://doi.org/10.1016/j.ijscr.2021.106137

[13] Hayes, A. (2022) Blockchain Facts. https://www.investopedia.com/terms/b/blockchain.asp

[14] Technologies, X. (2017) Blockchain Imperative for Educational Certificates. Xanbell Technologies.

[15] Haber, S. and Stornetta, W.S. (1991) How to Time-Stamp a Digital Document. Springer Berlin Heidelberg, 437-455.

[16] Nakamoto, S. (2008) Bitcoin: A Peer-to-Peer Electronic Cash System. https://www.bitcoin.org

[17] Zheng, Z., Xie, S., Dai, H., Chen, X. and Wang, H. (2017) An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends. *Proceedings of* 2017 *IEEE* 6*th International Congress on Big Data* (*BigData Congress*), Honolulu, 25-30 June 2017, 557-564. https://doi.org/10.1109/BigDataCongress.2017.85

[18] Ghazali, O. and Saleh, O.S. (2018) A Graduation Certificate Verification Model via Utilization of the Blockchain Technology. *JTEC*: *Journal of Telecommunication*, *Electronic and Computer Engineering*, **10**, 29-34.

[19] Dongre, J.G., Tikam, S.M. and Gharat, V.B. (2020) Education Degree Fraud Detection and Student Certificate Verification Using Blockchain. *IJERT*, **9**, 300-303. https://www.ijert.org

[20] Suganthalakshmi, M.R., Praba, M.G.C., Abhirami, M.K. and Puvaneswari, M.S. (2022) Blockchain Based Certificate Validation System. https://www.irjmets.com