Blockchain Based Academic Certificate Authentication System

Prof. Srinath G M
Asst .Prof, Dept.COMPUTER SCIENCE AND ENGINEERING
S.J.C Institute of Technology
Chickballapur,India
srinathgms88@gmail.com

Bhavana S
Student, Dept.COMPUTER SCIENCE AND ENGINEERING
S.J.C Institute of Technology
Chickballapur,India
bhavanasreddy10@gmail.com

Chandana B
Student, Dept.COMPUTER SCIENCE AND ENGINEERING
S.J.C Institute of Technology
Chickballapur,India
chandana.bb2001@gmail.com

Manoj R
Student, Dept.COMPUTER SCIENCE AND ENGINEERING
S.J.C Institute of Technology
Chickballapur,India
manojrajmanu2@gmail.com

Monish M
Student,Dept.COMPUTER SCIENCE AND ENGINEERING
S.J.C Institute of Technology
Chickballapur,India
monishmaruthi2016@gmail.com

Abstract— The graduation certificates issued by universities and other educational institutions are among the most important documents for graduates. A certificate is a proof of a graduate's qualification and can be used to apply for a job or other related matters. The advance of information technology and the availability of low-cost and high-quality office equipment in the market have enabled forgery of important documents. However, verification of certificates using traditional methods is costly and very time-consuming. Therefore, the goal of this proposed model that can offer a potential solution for academic certificate issuing and verification using blockchain technology. The proposed system uses SHA-256 algorithm to create a tamper-proof record of academic certificates and making it impossible to falsify or manipulate them. The system will also provide a decentralized platform for certificate verification, enabling employers, educational institutions, and other stakeholders to easily verify the authenticity of academic certificates.

Keywords—tamper-proof, authenticity, decentralized, SHA-256(Secure Hash Algorithm).

I. INTRODUCTION

Block chain is a distributed database or ledger that is shared among the nodes of a computer. As a database, a block chain stores information electronically in digital format. The immutable, decentralized and secure features of the blockchain increases trust, security transparency and traceability of data shared in the network. It maintains a decentralized and secure record of crypto transactions. The data is sensitive and crucial, and blockchain can significantly change how the critical information is viewed. By creating a record that cannot be altered and is encrypted end-to-end, blockchain helps to prevent fraud and unauthorized activity. Information is stored across a network of computers rather than a single sever, making it difficult for hackers to view data.

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]. There are currently 2 million fake degree certificates in circulation in the United States and 300 unauthorized universities operating [3]. A study shows that almost 10% of applications given by candidates are forged [4]. Applicants tend to lie about their education andexperience [5]. Every year, academic certificate fraud costs employers approximately $600 billion [6]. Certificate forging is also causing problems in themedical field. Many people pretend to be a doctor by forging fake certificates. As a result, people fromall socioeconomic backgrounds will not receive equal treatment when they visit different types of doctors [7].

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 blockand 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. Cybersecurity is the application of technologies, processes, and controls to protect systems, networks, programs, devices and data from cyber-attacks. It aims to reduce of cyber-attacks and protect against the unauthorized exploitation of systems, networks and technologies. 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. Most of the existing methods are time-consuming because they are labor-intensive, partially automated or involve human to human interaction. To overcome this, the project aims to develop academic certificate generation and verification system that employs the use of block chain technology and quick response code in providing security, simple and easy to use platforms for institutions, organizations or anyone concerned to verify the authenticity of educational certificates.

II. LITERATURE REVIEW

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.

Blockchain was introduced long before Bitcoin was introduced by Satoshi Nakamoto[8], [9]. However,blockchain gained its popularity with Bitcoin. Although bitcoin is sometimes referred to as a blockchain by somepeople, 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.

Jayesh G. Dongre and his colleagues proposed[10] 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 [11] and her colleaguesinvestigated an optimal method of verifying academic credentials in 2022. The number of graduating studentsis 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 interestedin building a system to verify and generate academic certificate. 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 certificate.

III. PROPOSED METHODOLOGY

The proposed models and its methodologies are predicted by performing the following steps:

1. System Design: The system design involves defining the architecture of the blockchain-based academic certificate authentication system, including the selection of a blockchain platform, such as Ethereum or Hyperledger, and the development of smart contracts for managing the issuance and verification of digital certificates.

2. Certificate Issuance: The certificate issuance process involves verifying the identity of the student and the completion of the academic program. Once verified, a digital certificate is generated and stored on the blockchain. The certificate includes information such as the student's name, the name of the academic program, and the date of completion.

3. Certificate Verification: The certificate verification process involves the use of a public key to verify the authenticity of the digital certificate. The public key is stored on the blockchain and is accessible to employers or other institutions who wish to verify the certificate.

4. Integration with Existing Systems: The blockchain-based academic certificate authentication system can be integrated with existing academic systems, such as student record systems and online learning platforms. This integration allows for seamless certificate issuance and verification processes.

5. Security and Privacy: The security and privacy of the system are paramount to ensuring the integrity of the digital certificates. The system should be designed to protect against cyber-attacks, data breaches, and unauthorized access to the blockchain. The system should also be designed to ensure the privacy of student information.

6. Testing and Evaluation: The system should undergo rigorous testing and evaluation to ensure that it functions as intended and meets the needs of the users. User acceptance testing should be conducted to gather feedback from students, employers, and educational institutions to ensure that the system is user-friendly and meets their needs.

IV. WORKFLOW OF PROPOSED SYSTEM

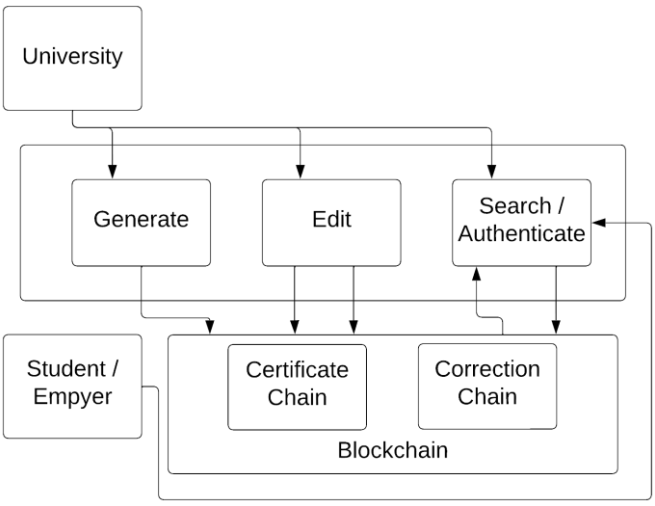

Figure 1: System Architecture

In this study, the general idea of the proposed system is depicted in Fig-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.

SHA-256: SHA-256 is a part of SHA-2 (Secure Hash Algorithm 2). It is a popular hashing algorithm. A cryptographic hash, known as a fingerprint, or signature,is a nearly identical string of characters generated froma different piece of input text. SHA-256 generatesa 256-bit signature. SHA-2 is widely known for its security (it hasn't weakened as much as SHA-1)

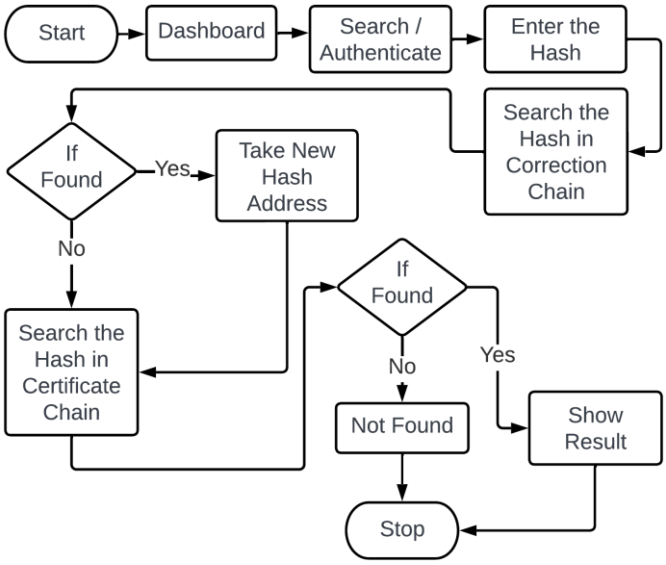

Figure 2: Checking the authenticity

The validation-checking process is shown in Fig-2. In our system, a certificate can be checked in two ways. This can either be done by manual typing or scanningthe QR code. QR code will contain the hash addressof 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.

V. RESULTS AND DISCUSSIONS

The Blockchain-Based Academic Certificate Authentication System project resulted in the development of a secure, efficient, and user-friendly system for issuing and verifying digital certificates using blockchain technology. The system provides a tamper-proof and decentralized method for certificate verification, ensuring that the certificates cannot be altered or counterfeited. User acceptance testing showed that the system was well-received by students, employers, and educational institutions, with users noting that the system was easy to use and provided a secure and efficient method for certificate issuance and verification.

The integration of the system with existing academic systems proved to be seamless and efficient, allowing for the easy issuance and verification of digital certificates without the need for manual processes. The scalability of the system was also demonstrated, allowing for the issuance and verification of a large number of digital certificates.

Privacy was maintained throughout the certificate issuance and verification process, with the use of public-private key cryptography ensuring that only authorized parties can access the digital certificates.

The Blockchain-Based Academic Certificate Authentication System project resulted in the development of a robust and secure system for managing digital certificates using blockchain technology. The system provides a solution for academic institutions and employers looking for a secure and efficient method for certificate issuance and verification, while ensuring the privacy of student information

VI. CONCLUSION AND FUTURE WORK

In conclusion, the Blockchain-Based Academic Certificate Authentication System project demonstrated the potential of blockchain technology in addressing the challenges associated with traditional certificate issuance and verification processes. The system developed in this project provides a secure, efficient, and user-friendly solution for managing digital certificates using blockchain technology.

Future work for this project includes further testing and evaluation to ensure the scalability and reliability of the system. The system can also be expanded to include additional features, such as the ability to store other academic records, including transcripts and diplomas. The integration of the system with other blockchain-based solutions, such as digital identity systems, can also be explored to enhance the security and privacy of the system.

The system can be further developed to include smart contracts that automatically validate certificates against certain criteria, such as expiration dates, to ensure their validity. This would provide an added layer of security and would reduce the risk of fraudulent certificate use.

REFERENCES

[1] T. Healy, S. Cote, J. Helliwell, and S. Field, "The Well-Being of Nations -The Role of Human and Social Capital," Oecd, p. 118, 2001

[2] S. Baum, J. Ma, and K. Payea, "Education Pays 2013," Coll. Board, pp. 1–48, 2013

[3] Greenleaf, A.; Kurylev, Y.; Lassas, M.; Uhlmann, G. (2007). "Improvement of cylindrical cloaking with the SHS lining".

[4] R. Garg, "Blockchain Ecosystem for Education & EmploymentVerification." 13th International Conference on Network & Communication Security. Toronto, Canada. 2021.

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

[6] E. ChiyevoGarwe, "Qualification, Award and Recognition Fraudin Higher Education in Zimbabwe," J. Stud. Educ., vol. 5, no.2, pp. 119–135, 2015.

[7] T. Ahmed, "The Case of Doctor-Patient Relationship in Bangladesh: An Application of Relational Model of Autonomy,"Bangladesh Journal of Bioethics, vol. 12, no. 1, pp. 14–24, Feb.2021, doi: 10.3329/bioethics.v12i1.51900

[8] S. Haber and W. S. Stornetta, "How To Time-Stamp a Digital Document I," 1991.

[9] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System." [Online]. Available: www.bitcoin.org

[10] J. G. Dongre and S. M. Tikam, "Education Degree Fraud Detection and Student Certificate Verification using Blockchain." [Online]. Available: www.ijert.org

[11] M. R. Suganthalakshmi, M. G. Chandra Praba, M. K. Abhirami, M. S. Puvaneswari, and A. Prof, "BLOCKCHAIN BASED CERTIFICATE VALIDATION SYSTEM." [Online]. Available:www.irjmets.com