2024 6th International Conference on Sustainable Technologies for
Industry 4.0 (STI), 14-15 December, Dhaka

Development of Blockchain-based Framework for Certificate Verification and Fraud Prevention

Md. Dulal Hossain[1], **Md.Rabby Khan**[1], Mostak Ahammad[1], Sudip Chandra Ghoshal[1], Md. Ahsan Habib[1,2]
[1]Department of Computer Science and Engineering, Green University of Bangladesh, Dhaka, Bangladesh
[2]Department of ICT, Mawlana Bhashani Science and Technology University, Bangladesh
Email: dulal.md.cse@gmail.com, rabbykhan80448044@gmail.com, mostakahmed5913@gmail.com,
sudip@cse.green.edu.bd, mahabib@cse.green.edu.bd

***Abstract*—Since the advent of digital technology in the era of 4th industrial revolution, authentication of professional and academic certificates has been a major challenge. Traditional verification is time-consuming, tedious, and expensive, and this is why the credentials are susceptible to counterfeiting with fraud and tampering. Therefore, this paper presents a blockchain-based framework for certificate verification that will ensure reliability, authinticity, transparency, and integrity of all forms of certificates. In this paper, it is used the Ethereum Smart Agreement to ensure the securely and authentication of certificates. Each academic certificate is washed with SHA-256 encryption and recorded in the blockchain, so that it becomes pref-tamper and real-time verifiable from anywhere in the world. Manual authentication can be confirmed using a distinct hash or QR code eliminating requirements. The process reduces the verification period from day to second and eliminates the dependency on the centralized database, which is generally targeted by cyber attacks. Therefore, the proposed system can prevent fraud and build a trusted digital certification system for any organization.**

***Index Terms*—Blockchain, Certificate Verification, Fraud Prevention, Smart Contracts, Ethereum, SHA-256, Digital Signatures.**

I. Introduction

In today's digital world, employment and educational certificates are the backbone in verifying an individual's qualification and expertise. The traditional methods of certificate issuance and verification are also prone to forgery such as certificate forgery, tampering, and identity theft. Moreover, the manual verification systems are time-consuming, costly, and prone to third-party verification, which causes inefficiencies along with security threats. To counteract such problems, blockchain technology presents a decentralized, transparent, and tamper-proof way of securing issuance and authentication of certificates.

Blockchain's immutable ledger and cryptographic security render it impossible, once committed, to tamper with or modify a certificate. Blockchain provides distributed trust instead of conventional centralized database approaches, and therefore cyberattacks and unauthorized modifications become less likely [1]. Further, the application of smart contracts provides automatic verification, along with certificate authentication anywhere and everywhere in the world instantly, without involving intermediaries [2].

Numerous studies in using blockchain in verification of certificates have been carried out. Rustemi et al. [**?**] examined systematically academic certificate verification systems supported by blockchain, nailing such key benefits as higher security, fraud reduction, and automatization. Similarly, KC et al. [3] also put forth a blockchain-based fake certificate detection system, emphasizing efficiency in guaranteeing authenticity. However, such drawbacks as scalability issues, outrageous transaction fees, and integrative complexity problems are an overhang [4].

Blockchain-based security applications are also gaining popularity. Ali et al. [4] proposed blockchain for security in IoT-based systems, while Zhang and Wen [9] discussed its use for networked system security. In the context of Industry 4.0, Rahman et al. [5] proposed AI-powered blockchain models for APT countermeasure and demonstrated the efficacy of blockchain for digital infrastructure security.

In this research, a Blockchain-Based Certificate Authentication and Preventing Fraudulent Activities System is presented, where Ethereum smart contracts, SHA-256 hashing, and QR-code authentication are utilized. Our system concentrates on:

- Prevention of forgery of certificates through immutability.
- Shifting verification time from days to seconds.
- Allowing global access regardless of any central authority.
- Raising automation by using smart contract-based verification.

By bridging current gaps and aggregating successful, cost-effective, and scalable blockchain technologies, this effort seeks to contribute to the establishment of a secure, standard, and universally accepted certificate verification system.

II. Preliminaries and Related Works

The blockchain technology has been a groundbreaking answer to the security of online transactions and data verification, especially in the Internet of Things (IoT), cybersecurity, and certificate verification. There has been abundant research on the use of blockchain in these fields in the pursuit of greater security, decentralization, and transparency.

Sun et al. [[1] also proposed a blockchain-based access control mechanism in IoT scenarios with assurances of cross-domain and lightweight secure solutions. Their solution remedies security vulnerabilities in IoT devices through the

979-8-3315-3197-3/24/$31.00 ©2024 IEEE

use of blockchain for decentralized authentication. Likewise, Aloqaily et al. [2] proposed a lightweight and decentralized authentication protocol for IoT networks with emphasis on resource-aware consumption and enhanced security. Both articles report the potentials of blockchain for IoT network security.

KC et al. proposed a blockchain-based approach to identify counterfeit physical certificates through an issuer verification system. Their approach has achieved lower fraud cases while still maintaining certificate integrity and authenticity. The utilization of Rustemi et al.'s [4] method of classifying available solutions along with existing research gaps allowed for a systematic survey on the blockchain-based authentication of academic certificates to be conducted. Jadhav et al. [3] also analyzed the use of blockchain in tamper-proof and secure storage of certificates for authentication purposes. All these papers confirm that indeed the use of blockchain technology can prevent forgery of certificates.

In the wider context of cybersecurity, Zhang and Wen [6] presented a blockchain-oriented cybersecurity framework to solve security concerns in networked distributed systems. Dehghantanha and Choo [7] spoke of blockchain-enabled IoT cybersecurity systems and showed blockchain's use in stopping cyber-attacks. Wang et al. [8] presented a new way of storing data in IoT devises securely using secret-sharing techniques and a collaborative blockchain to ensure confidentiality and reliability, as well as decentralized cloud storage systems. Rahman et al. [**?**] integrated blockchain and artificial intelligence for Industry 4.0 Cyber-Physical System security against advanced persistent threats.

All these research contributions together underscore the significance of blockchain for enhancing security, authentication, and data integrity in general in industries. The present research contributes value to these research contributions by proposing a more efficient blockchain-based certificate verification system as a niche solution for certificate authentication and fraud elimination problems.

A. Existing System:

In the traditional certificate authentication system, institutions issue paper-based or digital certificates that require manual verification. These systems are often victims of security risks, inefficiency and fraud.

1) Drawbacks of the Current System:: Lack of assistance for certificate verification.

III. LITERATURE REVIEW

A. Blockchain and Smart Contract for Digital Certificates:

As per data from the In 2015 the New York Times reported on a billion-dollar industry consisting of 3 300 "diploma mills". These were fake universities that sold certificates for all levels of degrees, worldwide. Bangladesh Ministry of Education, around 900,000 students graduate annually, with some opting for further education abroad, in high schools, or tertiary institutions, while others prepare for employment or seek job placements. During the course of schooling, students' achievements such as conduct awards, academic transcripts, diplomas, etc., become crucial references for admission to new schools or careers. When schools issue different honors or diplomas, usually only the names of the schools and students are documented. When schools administer sundry accolades or diplomas, merely the designations of schools and pupils are recorded. Because there isn't a strong anti-forgoing system in place, stories regarding graduation certificate fraud frequently surface. To address the issue of counterfeit certificates, the blockchain-based digital certificate system is put forth. The unchangeable nature of blockchain facilitates the creation of digital certificates with verification and anti-counterfeit capabilities. In such a setup, the procedure for distributing digital certificates proceeds as follows: Firstly, while computing the hash value for this electronic record, an electronic record of the paper certificate is stored in the database along with any relevant additional data. Subsequently, this hash value is inserted into a blockchain block for safekeeping. The system generates both a QR code and a query sequence code that can be attached to the paper certificate. This will enable the recipient to verify the authenticity of the paper certificate through mobile phone scanning or online queries. It shall furnish the requesting entity with the capability to authenticate the legitimacy of the paper certificate via mobile phone scanning or website interrogations. Due to the immutable characteristics of blockchain, the system not only enhances the trustworthiness of numerous paper-based certificates but also digitally minimizes the risk of various certificate losses.

B. Blockchain-Based Decentralized System for Certificate Revocation:

Existing approaches to revoking digital certificates prove inadequate in scenarios involving multiple certification authorities (CAs), resulting in a deficiency of mutual trust, access reliability, and timely data synchronization among CAs. We propose a decentralized approach to digital certificate cancellation using a combination of secret-sharing and consortium blockchain technologies. In certain cases, this method may render the digital certificate ineffective, safeguarding user information and property security. Consortium blockchain technology, which takes advantage of decentralized consensus processes, is the core of the system. Once this system successfully enables collaborative management of digital certificate revocation lists (CRLs) across multiple Certificate Authorities (CAs) and incorporates a secret sharing scheme, it could lead to the creation of an Online Certificate Status Protocol (OCSP). This advancement increases the maintenance process's reliability and makes the system safer, resilient, and resistant. Unlike traditional revocation methods, this innovative solution creates a robust and credible Certificate Revocation List (CRL) system that is shared by several certification authorities (CAs). A system like this could open up new perspectives on the revocation of digital certificates and expand the range of uses for blockchain technology.

C. Certificate Verification System using Blockchain:

For quite some time, there has been a significant issue with the proliferation of fraudulent certificates. The drive for individuals to secure employment has led to the commercialization of certificate issuance.. Since the holders of these phony credentials deny them what may be theirs, hardworking individuals with valid degrees or certifications must bear the repercussions of this phenomena. This may often prove to be quite harmful. Imagine a situation in which a surgeon performs surgery based only on a fake degree. Such incidents highlight how crucial it is to have a system that can authenticate and validate certificates, as well as the holders and issuers of them. In this paper, we present a methodology that takes benefit of the tamper-proof and non-repudiation properties offered by blockchain technology to facilitate the issuance and validation of certificates.

IV. METHODOLOGY

1) **Issuing User Certificates:**
Users can obtain credentials from their affiliated universities or government bodies via the Ethereum infrastructure.
2) **Blockchain Storage:**
In order to achieve security and immutability, every user has a digital locker on the Ethereum blockchain where smart contracts can be applied to store the user's certificates.
3) **Create Unique URL/QR Code:**
Each user has a unique detector with the certificate, in the form of a URL or QR code, which points to their certificate in the blockchain.
4) **Distribute Certificate:**
URL or QR codes created by users distribute to the agencies and individuals that need to be for authentication.
5) **Organization Verification:**
Organizations can access the webpage and commence the validation process with the URL or QR code provided by the user.
6) **Validation:**
The validation process verifies the issued certificate can be authenticated. The system confirms certificates by checking on the blockchain information related to the provided URL or QR code.

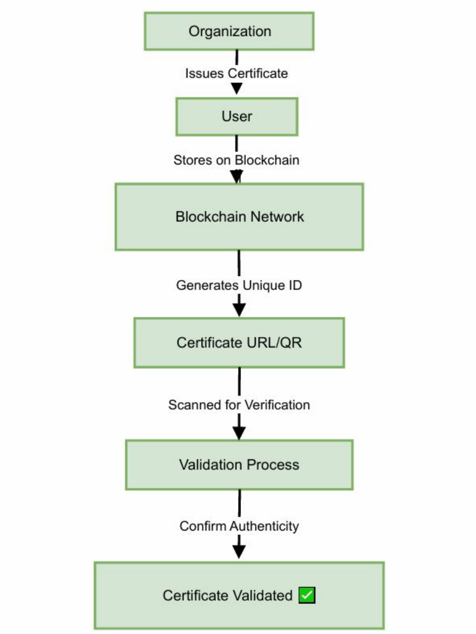

Fig. 1: Methodology Process for Development of Blockchain-based Framework for Certificate Verification and Fraud Prevention

A distributed, decentralized database is what blockchain is. The following are the procedures by which the system created in this study operates: Schools offer degree certificates in addition to submitting the student's data into the system. The student's serial number is then immediately logged onto a blockchain by the technology. The certificate system verifies all of the data. Instead of typical paper copies, schools award e-certificates with a rapid response (QR) code to graduates whose data has been properly authenticated. Every graduate also receives an inquiry number and an electronic file for their certificate. When seeking for a job, a graduate only needs to email the target firms their e-certificate with a QR code or their serial number. When businesses reach out to the system wfoith inquiries, it lets them know if the serial numbers are authentic. The QR code lets them to check whether the certificate has been tampered with or is fraudulent.

The system suggested utilizing its own private blockchain to create dynamic certificates in a novel way. The first step is for the student to apply online for an e-certificate and submit all of their academic records. Web portal is an accredited, reliable third party that verifies all university, college, and school paperwork, among others. The technology creates a unique certificate ID or QR code, stores the data on a blockchain, and sends the data back to the student following a successful verification process conducted by a university, college, or school. Students can give the organization their certificate ID or assigned QR code in place of sending hard copies of the paperwork. Through the site, organizations can gather the associated student's e-certificates, authenticate them, and upload their IDs or QR codes. We created a smart contract on the blockchain to streamline the entire process. We conducted tests to assess the proposed system's resistance against different types of network assaults, including Man-in-the-Middle (MiM) and Denial-of-Service (DoS) attacks, as well as to test it in a susceptible setting. For every student's paper, the suggested method creates a distinct certificate and dynamic QR code. Data e-certificates that are securely held on the blockchain increase security. The smart contract technology permits modifications throughout the blockchain, according to this as well. This research recommended a custom blockchain development using an open-source framework.

V. PROPOSED SYSTEM

Therefore, we are presenting blockchain technology in our proposed paper, which stores immutable data that cannot be altered in any way. Therefore, upon storing a copy of the certificate on the blockchain and retrieving it, the administrative user will generate a QR code using the certificate's digital signature and attach it to the student's certificate. This certificate can be scanned by other companies or organizations to verify and retrieve data from Blockchain. If QR-CODE is included in the blockchain, then the certificate validation procedure will be successful.

A. The Advantage of the Proposed System

Self-performing agreements, known as ”Smart Contract”, are composed of a clear agreement that is encoded in code. They work on the blockchain system, such as Ethereum, and when the specific criteria are met, they automatically execute and apply the terms of an agreement. Smart agreements are a game-changing discovery in several industries, including supply chain management, legal procedures and banking, because they are tamper-proof, safe and decentralized.

1) **Modern and Relevant:**
The current project maintains the currency and value of the certificate in the current digital age. It is in line with the contemporary approach.
2) **Certificate Cannot Be Changed:**
Certificates can't be changed or faked after saving in blockchain. Ensures certifications are always authentic.
3) **Save Money:**
Due to the reduction of the amount of assets required for papers and manual checks, businesses and schools can save money. As a result, it can be enough to afford time.
4) **Fast Certificate Provision:**
Businesses and universities can provide direct certificates in blockchain, thereby eliminating the need for documentation. It accelerates the certification process.
5) **Transparency and Trust:**
The protected record of each step in the creation and verification process is kept. It maintains accountability and increases confidence.
6) **Simple Verification:**
People can use a specific URL or QR code to quickly verify that certificates are authentic. It's easy and fast.
7) **Reliable Verification:**
Providing a uniform and reliable method of certificate verification for our technology companies makes it easy to distinguish between the original and fake certificate.
8) **User-Friendly:**
We have made our system user-friendly for all. It will be easy &clear for those who have credentials & those who verify.
9) **Advanced Safety:**
Our solution uses blockchain technology, which is incredibly secure and almost impossible to hack. It shows that certificates are safe against manipulation and illegal use.

VI. IMPLEMENTATION

Nowadays, everyone chooses to pursue education in order to land a decent career. In order to do this, individuals are creating phony diplomas, which cannot be verified by current technologies. Therefore, we are presenting blockchain technology in our proposed paper, which stores immutable data that cannot be altered in any way. Therefore, the admin user will create a QR code based on the digital signature on the certificate and attach it to the student's certificate after storing a copy of the certificate in the blockchain and obtaining it. Other businesses or organizations can scan this certificate to confirm and retrieve information from Blockchain. The certificate validation process will be successful if QR-CODE is present in the blockchain.

A. Blockchain Technology Overview

A distributed data storage system called blockchain makes it feasible to verify data using hash codes. It creates a peer-to-peer network in which several peers duplicate the data kept in a single peer. Within the blockchain, every data block is represented by a distinct hash code. Blockchain verifies previous hash codes before saving new records. If all hash codes match across nodes, new records are stored; if not, the data is deemed tampered with. As a result, blockchain data is difficult for third parties to alter, which is why it is called immutable.

VII. CONCLUSION

Data security stands as a fundamental aspect of blockchain technology. The blockchain acts as an extensive, open-access online ledger in which every node stores and verifies the same data. The proposed blockchain-based method significantly decreases the likelihood of certificate forgery. Moreover, the system's automated certificate issuance and application processes ensure transparency and openness. Thus, companies or groups are able to ask the system questions respecting any certificate. To sum up, the information is precise and private thanks to the system.

ACKNOWLEDGMENT

This work was supported in part by the Center for Research, Innovation, and Transformation of Green University of Bangladesh.

REFERENCES

[1] S. C. Shengling Sun, Ruoyu Du and W. Li, “Blockchain-based iot access control system: Towards security, lightweight, and cross-domain,” *IEEE Access*, 2021.

[2] M. Aloqaily, S. Otoum, Y. Jararweh, and I. Al Ridhawi, “A decentralized lightweight blockchain-based authentication mechanism for iot systems,” *Cluster Computing*, 2020.

[3] A. KC, A. Shrestha, S. Shrestha, and S. Shakya, “Detection of fake physical certificates using a blockchain-based certificate verification and issuer validation system,” *2023 2nd International Conference on Computing and Communication for Smart World (I3CS)*, pp. 1–6, 2023.

[4] A. Rustemi, F. Dalipi, V. Tanaskovski, and A. Risteski, "A systematic literature review on blockchain-based systems for academic certificate verification," *IEEE Access*, vol. 11, pp. 123 456–123 470, 2023.

[5] Z. Rahman, X. Yi, and I. Khalil, "Blockchain-based ai-enabled industry 4.0 cps protection against advanced persistent threat," *IEEE Internet of Things Journal*, vol. 10, no. 8, pp. 6769–6778, 2023.

[6] B. Jadhav, N. Maharnawar, R. Lakhotiya, R. Malpani, V. Ligde, and P. Savale, "Blockchain-based certificate verification," *Proceedings of the 1st International Conference on Cognitive Computing and Cyber Physical Systems*, 2024.

[7] Y. Zhang and J. Wen, "A blockchain-based cyber-security for connected networks," *Transactions on Emerging Telecommunications Technologies*, vol. 29, no. 4, 2018.

[8] M. C. Ali Dehghantanha and K.-K. R. Choo, "Cybersecurity for blockchain-based iot systems: A review," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 8, pp. 3723–3735, 2018.