Grenze International Journal of Engineering and Technology, June Issue

A Blockchain Based Certificate Verification

Sanjay Pande[1], Ahefaz Sheikh[2], Mitesh Dhanore[3], Rushikesh Nagare[4] and Devang Kakde[5]
[1] Assistant Professor, Yeshwantrao Chavan College of Engineering, Wanadongri, Nagpur, India.
[2-5]Final year students, Department of Computer Technology, Yeshwantrao Chavan College of Engineering, Wanadongri, Nagpur, India.
Email: ahefazsheikh02@gmail.com

***Abstract*— A major challenge in universities is verifying the authenticity of certificates generated each year when students graduate. False academic credentials are becoming increasingly common all over the world. Many strategies to combat this scourge have proven ineffective and fall short of modern techniques used in academic fraud. Currently, there is no reliable mechanism to validate these certificates, leading to widespread forging and use of fake certificates in the job market. This study aims to investigate the problems in the current certificate verification systems in universities and to propose a solution by implementing a secure, permissioned blockchain-based certificate verification system. The system would utilize blockchain to issue & verify certificates, providing an anti-forgery mechanism for managing certificates that cannot be altered. To address this issue, a decentralized web app has been created that registers certificates on blockchain and uses a smart contract to validate their authenticity. The proposed system is a blockchain-based solution for registering student information and storing digital certificates. It includes an administrator login, student and certificate addition, and verifier page. The system allows for verification of certificates by employers or verifiers by providing the student's information and checking the hash value using QR code.**

***Index Terms*— Blockchain, Decentralized, Smart Contract, Hash.**

I. INTRODUCTION

Each year, many students finish their studies and proceed to graduate school or find employment in the corporate world. In this situation, the process of document verification is used to confirm the student's credentials. As a result of a missing secure method to prevent counterfeiting, graduation certificates can be falsified when they are being reviewed during transfer between schools. Due to the high cost and effort involved in verifying the credentials of incoming employees, a digital certificate system using blockchain technology has been proposed as a solution. Blockchain is a decentralized digital ledger that is collectively maintained by a network of computers, ensuring the security and immutability of the data as it cannot be altered by a single entity without the approval of all participants in the network. Technologies exist in related fields that are utilized in e-documents to offer authentication and integrity, such as digital signatures. While digital signatures meet the standards for electronic qualification certificates, they have major security vulnerabilities and lack certain features. For instance, it uses the keys to confirm document modifications but does not automatically begin validating the state of public key certificates. If the key has been compromised, this can lead to a forgery being recognized. Furthermore, the signed document has been validated along with the signer's public key certificate, not the actual document. This project aims to create a secure blockchain-based verification system for academic certificates, where permissions are controlled, and certificates can't be altered. The use of blockchain technology can reduce the cost and time it takes

Grenze ID: 01.GIJET.9.2.111

to verify documents from weeks to mere seconds, allowing students to selectively share their certificates without making them public. This is achieved through the implementation of a private blockchain.

II. Literature Survey

Blockchain technology has gained significant attention in various domains due to its decentralized and transparent nature. In the realm of document authentication and verification, several researchers have explored the potential of blockchain-based solutions. This literature review examines the existing research papers that propose different approaches and applications of blockchain technology for document authentication and related areas.

Latha et al. [2] introduced a decentralized application that allows users to upload and authenticate documents using a unique hash. Their implementation utilized the Ethereum test net Ropsten, smart contracts, and SHA256. The system provided transparency, security, and immutability without the involvement of third parties. Similarly, Hrithik Gaikwad et al. [3] designed a decentralized application using the Ethereum blockchain service and the Rinkeby test network. Their solution incorporated smart contracts, a web app, and the Truffle framework, ensuring incorruptibility, encryption, and data synchronization. T.S.Raja Rajeswari et al. [4] proposed a system where the hash generated during block creation serves as a "hash-key" for retrieving the original document from the blockchain. They employed SHA-256 for hash generation and utilized test ether for transactions due to the high cost of original ether. Another study by Guang Chen et al. [5] focused on preventing plagiarism in educational contexts. They proposed a blockchain-based solution that employed private blockchain platforms hosted by each institution, aiming to lower transaction costs and facilitate implementation. However, challenges were identified, such as the need for teachers to use the blockchain platform for validation and the difficulty of conducting accurate assessments online.

Niranjanamurthy et al. [6] discussed the potential of blockchain technology for digital asset interchange in various domains, including contracts, money, services, and medical and educational data. Their proposed system leveraged a peer-to-peer network and eliminated the reliance on a central authority for trust. S. Smys et al. [7] utilized Hyperledger Fabric to support private blockchains that combined online ledgers and offline CouchDB. Their system stored mutable data in CouchDB and immutable data, such as certificates, on a digital ledger through chain code, providing scalability and a permissioned architecture suitable for industrial applications.

Haibo Yi [9] introduced a blockchain-based e-voting scheme that fulfilled the necessary requirements of the e-voting process. The scheme employed hash values in the blockchain to link each vote securely. Raghav et al. [12] proposed a system for certificate management, where a trusted entity could input user information into a web portal and upload the resulting certificate to the IPFS network. V. Aleksieva et al. [13] addressed the challenge of smart contract migration across multiple channels with separate business logic. They proposed a solution for fast and secure migration, ensuring confidentiality between channels.

Performance comparison between blockchain platforms was explored by M. Dabbagh et al. [14]. Their experiments revealed that Hyperledger Fabric outperformed Ethereum in terms of success rate, average latency, throughput, and resource consumption. S. Huang [15] designed a platform utilizing RSA encryption for academic records and generating private keys for decrypting the encrypted data stored on the blockchain. D. Liu et al. [16] leveraged Kafka as a message queue for faster transaction processing. Their tests demonstrated that their scheme outperformed existing blockchain-based systems in terms of transaction speed. Devdoot Maji et al. [17] developed a system that involved an issuing authority, a hashing algorithm, and storage of document values. The security of the system was enhanced by employing asymmetric encryption and public hash keys.

M. Bahrami et al. [18] utilized smart contracts to decentralize essential services in the certification process, resulting in improved dependability, accuracy, privacy, and fault tolerance.

III. Methodology

This section presents the methodology used to design and implement the blockchain-based system for certificate authentication and verification. The system consists of three main pages: administrator login, student and certificate addition, and verifier page. The overall high-level design of the system is illustrated in Figure 1. The first step in the methodology involves the institution registering the student's information, including name, batch, department, CGPA, date of birth, and college. The certificate details, issued by the university, are stored within the blockchain along with the hash value, timestamp, and the hash value of the previous block. This ensures the immutability and integrity of the certificates.

The system allows administrators to log in using their credentials and add students and certificates to the database. The administrator login page provides access to the administrative features of the system. Once logged in, the

administrator can input the student's information and generate a certificate using a form, as shown in Figure 3. The generated certificate contains a unique ID printed at the bottom.

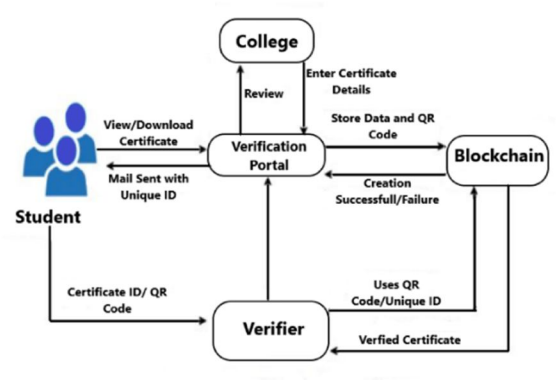

Figure 1. High Level Design

The application consists of three main pages: administrator login, student and certificate addition, and verifier page. The administrator can access the system using their login credentials to add students and certificates to the database. The verifier can log in and authenticate the certificate by providing the student's login ID and selecting the type of certificate. If the certificate is valid, the result will be "Authentic". If it has been altered, the result will show "invalid certificate". As part of the Recruitment, the Employer can utilize it to verify certificate and take legal action against any fakes. Blockchain network is permitted, which means that all participants must be verified and authenticated before they can join the blockchain.
Each block in the blockchain consists of the following information:

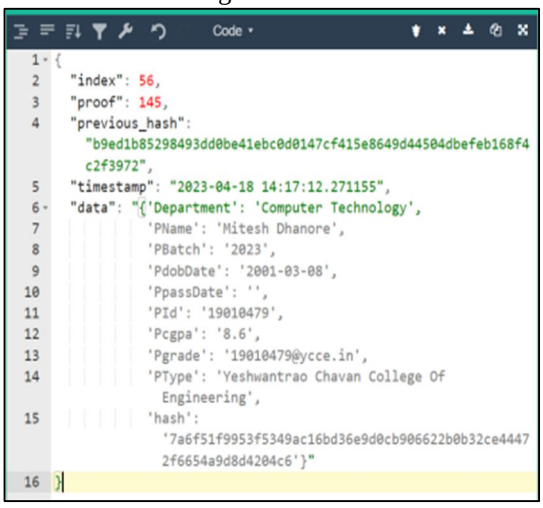

Figure 2. Example block.

IV. Result And Discussion

The Certificate issuer will only be able to generate certificates. The student can download his/her Document, and the Validator will be able to validate and view the document. So, each actor has their own features and doesn't have access to the features they do not need.
Certificate Issuer: The Certificate issuer has options to generate certificate by entering details in a form to generate a single certificate.
The document will be generated with its unique ID printed at the bottom of the document. After successful generation of certificate, the respective student is sent a mail with their certificate id.
Validator The Validator is the organization's authority who will need to validate the originality of the document when a student comes for admission. He will have two options – Validate using uploading QR, validate by entering ID.

1] Validate using ID The authority can insert or type in the unique ID for the document which he wants to validate.

If the ID matches the ID stored in the Blockchain a preview of the Document is generated along with basic details. If a fake ID is given an error is raised.

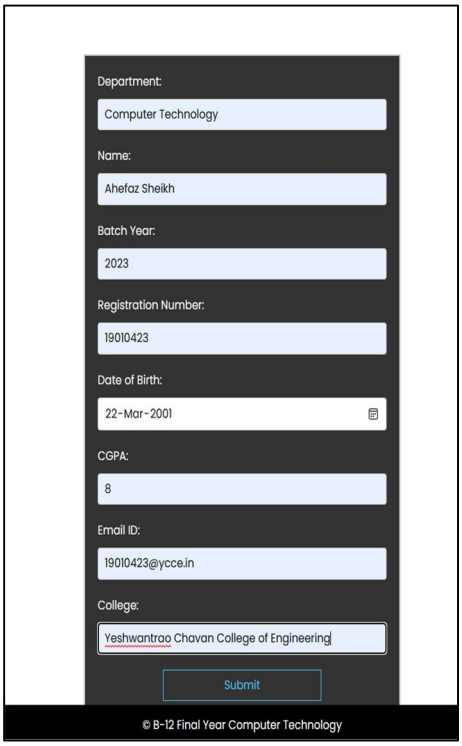

Figure 3. Filling of details for generating Certificate.

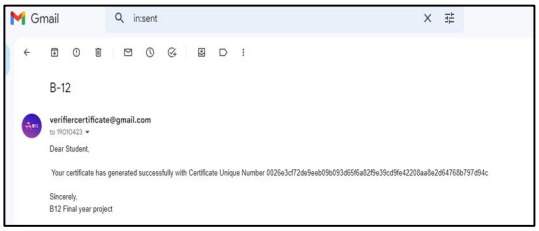

Figure 4. Mail sent to the student.

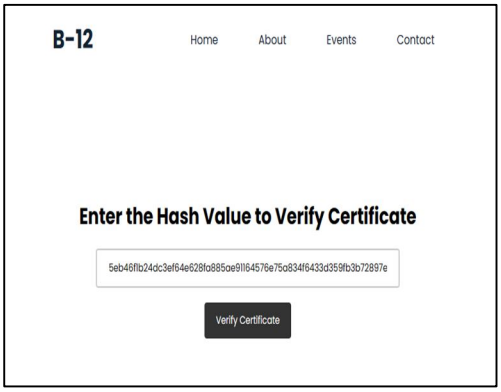

Figure 5. ID input being given for validation.

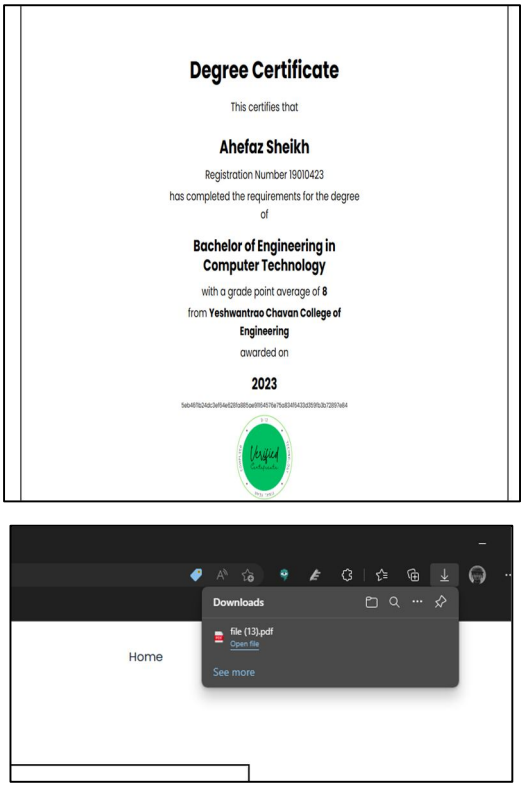

Figure 6. Successful Verification of Document generates preview and prints the Certificate.

Figure 7. An invalid Certificate ID being rejected.

2] Validate by Uploading QR

Another option for the validator is to directly upload the QR to the system. The hashed is extracted and matched with the hash stored in Blockchain and depending on the matching output is forwarded i.e., Valid, or Invalid
On Admin page, an administrator can check the validity of all nodes and data to ensure that the information has not been tampered with. The admin can view all the records, personal and verifier's starting from the first visit to the latest visit to all the verifiers.

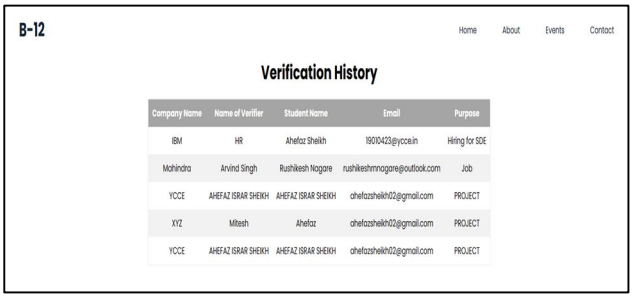

Figure 8. Verification History

The admin can view all the records, personnel and verifiers starting from the first visit to the latest visit to all the verifiers as shown in Figure.

V. Conclusion

As the number of fake certifications grows rapidly, it has become easier for unskilled people to utilize them to meet their needs. Credential fraud is a widespread and pervasive practice that undermines confidence in educational institutions, impairs social development, and involves significant economic costs. Any process involving education, such as applying for a job or needing identification, includes document verification as a requirement. So, a reliable verification system is required to verify certificates, of course. Unfortunately, legacy credential verification systems are time consuming, costly, and cumbersome. Moreover, they are not very effective against certain widespread corrupt practices, including fraud on the part of educational institutions and accreditation bodies.

Creating immutable ledgers is one of the main values of Blockchain. This behavior 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. The generated unique ID for each transaction is later used to verify the certificates. Thus, businesses and organizations can inquire for the verification of information of the certificate with QR code or Unique serial number.

References

[1] T. S. R. Rajeswari, S. K. Shareef, S. Khan, N. Venkatesh, A. Ali and V. S. Monika Devi, "Generating and Validating Certificates Using Blockchain," 2021 6th International Conference on Communication and Electronics Systems (ICCES), 2021, pp. 1048-1052, doi:10.1109/ICCES51350.2021.9489105.

[2] M. L. S. S, M. P. N and M. A. Shettar, "Block chain Based Framework for Document Verification," 2022 2nd International Conference on Artificial Intelligence and Signal Processing (AISP), 2022, pp. 1-5, doi: 10.1109/AISP53593.2022.9760651.

[3] H. Gaikwad, N. D'Souza, R. Gupta and A. K. Tripathy, "A Blockchain-Based Verification System for Academic Certificates," 2021 International Conference on System, Computation, Automation and Networking (ICSCAN), 2021, pp. 1-6, doi: 10.1109/ICSCAN53069.2021.9526377.

[4] Z. Wang, J. Lin, Q. Cai, Q. Wang, D. Zha and J. Jing, "Blockchain-Based Certificate Transparency and Revocation Transparency," in IEEE Transactions on Dependable and Secure Computing, vol. 19, no. 1, pp. 681-697, 1 Jan.-Feb. 2022, doi: 10.1109/TDSC.2020.2983022.

[5] A. Gayathiri, J. Jayachitra and S. Matilda, "Certificate validation using blockchain," 2020 7th International Conference on Smart Structures and Systems (ICSSS), 2020, pp. 1-4, doi: 10.1109/ICSSS49621.2020.9201988.

[6] Niranjanamurthy, M., Nithya, B.N. & Jagannatha, S. "Analysis of Blockchain technology: pros, cons and SWOT". Cluster Comput 22 (Suppl 6), 14743–14757 (2019).

[7] Smys, Smys & Haoxiang, Wang. "Data Elimination on Repetition using a Blockchain based Cyber Threat Intelligence." IRO Journal on Sustainable Wireless Systems 2021, 10.36548/jsws.2020.4.002.

[8] M. Li et al., "CrowdBC: A Blockchain-Based Decentralized Framework for Crowdsourcing," in IEEE Transactions on Parallel and Distributed Systems, vol. 30, no. 6, pp. 1251-1266, 1 June 2019, doi: 10.1109/TPDS.2018.2881735.

[9] Yi, H. "Securing e-voting based on blockchain in P2P network." Wireless Com Network 2019, 137 (2019). doi :10.1186/s13638-019-1473-6.

[10] K. Kumutha and S. Jayalakshmi, "Hyperledger Fabric Blockchain Framework: Efficient Solution for Academic Certificate Decentralized Repository," 2021 Fifth International Conference on ISMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), 2021, pp. 1584-1590, doi: 10.1109/ISMAC52330.2021.9640785.

[11] T. Kanan, A. T. Obaidat and M. Al-Lahham, "SmartCert BlockChain Imperative for Educational Certificates," 2019 IEEE Jordan International Joint Conference on Electrical Engineering and Information Technology (JEEIT), 2019, pp. 629-633, doi: 10.1109/JEEIT.2019.8717505.

[12] Raghav, N. Andola, R. Verma, S. Venkatesan and S. Verma, "Tamper-Proof Certificate Management System," 2019 IEEE Conference on Information and Communication Technology, 2019, pp. 1-6, doi: 10.1109/CICT48419.2019.9066236.

[13] V. Aleksieva, H. Valchanov and A. Huliyan, "Implementation of Smart-Contract, Based on Hyperledger Fabric Blockchain," 2020 21st International Symposium on Electrical Apparatus & Technologies (SIELA), 2020, pp. 113-116, doi: 10.1109/BIA50171.2020.9244500.

[14] M. Dabbagh, M. Kakavand, M. Tahir and A. Amphawan, "Performance Analysis of Blockchain Platforms: Empirical Evaluation of Hyperledger Fabric and Ethereum," 2020 IEEE 2nd International Conference on Artificial Intelligence in Engineering and Technology (IICAIET), 2020, pp. 1-6, doi: 10.1109/IICAIET49801.2020.9257811.

[15] S. Huang, "Academic Records Verification Platform Based on Blockchain Technology," 2020 International Conference on Computer Science and Management Technology (ICCSMT), 2020, pp. 203-206, doi: 10.1109/ICCSMT51754.2020.00048.
[16] D. Liu and X. Guo, "Blockchain Based Storage and Verification Scheme of Credible Degree Certificate," 2019 2nd International Conference on Safety Produce Informatization (IICSPI), 2019, pp. 350-352, doi: 10.1109/IICSPI48186.2019.9095961.
[17] Devdoot Maji , Ravi Singh Lamkoti , Hitesh Shetty , Bharati Gondhalekar, 2021, Certificate Verification using Blockchain and Generation of Transcript, International Journal of Engineering Research &Ttechnology (IJERT) Volume 10, Issue 03 (March 2021).
[18] M. Bahrami, A. Movahedian and A. Deldari, "A Comprehensive Blockchain-based solution For Academic Certificates Management Using Smart Contracts," 2020 10th International Conference on Computer and Knowledge Engineering (ICCKE), 2020.
[19] Vipul Badhe, Pooja Nhavale, Sonal Todkar, Prajakta Shinde, Prof. Kiran Kolhar, "Digital Certificate System for Verification of Educational Certificates using Blockchain," International Journal of Scientific Research in Science and Technology (IJSRST), Online ISSN : 2395602X, Print ISSN : 2395-6011, Volume 7 Issue 5, pp. 45-50, September-October 2020.
[20] T. Imam, Y. Arafat, K. S. Alam and S. A. Shahriyar, "DOC-BLOCK: A Blockchain Based Authentication System for Digital Documents," 2021 Third International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV), 2021, pp. 1262- 1267, doi: 10.1109/ICICV50876.2021.9388428.
[21] P. Soares, R. Saraiva, I. Fernandes, A. Neto and J. Souza, "A Blockchain-based Customizable Document Registration Service for Third Parties," 2022 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), 2022, pp. 1-2, doi: 10.1109/ICBC54727.2022.9805500.