Blockchain: Safeguarding Against Fake Degree Certificates in Bangladesh

*Securing Bangladeshi Education with Blockchain

1st Azizul Islam Nayem
Department of CSE
United International University
United City, Dhaka 1212, Bangladesh.
anayem201262@bscse.uiu.ac.bd

2nd Md Mushfikur Talukdar
Department of CSE
United International University
United City, Dhaka 1212, Bangladesh.
mtalukdar201056@bscse.uiu.ac.bd

3rd Sanjida Yesmin Ritu
Department of CSE
United International University
United City, Dhaka 1212, Bangladesh.
sritu191016@bscse.uiu.ac.bd

4th Jannat Wa-Sifat Meem
Department of CSE
United International University
United City, Dhaka 1212, Bangladesh.
jmeem191012@bscse.uiu.ac.bd

5th Sadia Hassan
Department of CSE
United International University
United City, Dhaka 1212, Bangladesh.
shassan191215@bscse.uiu.ac.bd

6th Mir Moynuddin Ahmed Shibly
Department of CSE (Lecturer)
United International University
United City, Dhaka 1212, Bangladesh.
moynuddin@cse.uiu.ac.bd

***Abstract*— In Bangladesh, the proliferation of counterfeit degree certificates poses a significant challenge to the authenticity of academic qualifications. To address this issue, we have developed a robust solution harnessing the power of blockchain technology. Our implemented solution leverages blockchain's inherent immutability and transparency to create a tamper-proof repository of educational credentials. By recording and verifying each degree certificate on the blockchain, we establish a secure and decentralized system that ensures the integrity of academic records. The implemented system showcases impressive performance in terms of accuracy and efficiency. With real-time verification capabilities, educational institutions and employers can quickly validate the authenticity of degree certificates, reducing the risk of accepting fraudulent credentials. This innovative approach not only safeguards the educational landscape but also streamlines the verification process, offering a reliable means to combat the menace of fake degree certificates.**

***Index Terms*—blockchain, safeguards, detection, cryptography, fake, certificates.**

I. INTRODUCTION

In the realm of higher education, the pursuit of knowledge and academic excellence is a cornerstone of personal and societal progress. However, the noble pursuit of education has been tainted by a rising concern: the proliferation of fake degree certificates. In Bangladesh, this issue has reached alarming proportions, casting a shadow over the credibility of educational qualifications and causing significant challenges for individuals, institutions, and the economy at large. There are issues with the current verification and issuance processes for academic certifications that revolve around the idea of trust. Their reputation and brand are damaged when fake certificates are issued in the name of educational institutions. Potential candidates' academic credentials cannot be swiftly or economically confirmed for legitimacy and authenticity. [6] Numerous instances of misbehavior by dishonest parties have taken place as a result of this gap. Over the past decade, instances of individuals presenting counterfeit degree certificates for academic and employment opportunities have surged. According to a report by The Daily Star, one of Bangladesh's leading newspapers, more than 6,000 fake degree certificates were uncovered in a single year, illustrating the extent of this problem "Over 6,000 Fake Certificates Found in One Year", The Daily Star, July 2019 [8]. Blockchain concepts have found applications across diverse fields, including sensor networks, the Internet of Things (IoT), smart urban infrastructure, healthcare management, education systems, and beyond. These innovative frameworks hold the potential to revolutionize established industries and create novel solutions. In an era of rapid technological advancement, blockchain's versatility continues to inspire new approaches that enhance transparency, security, and collaboration [7].

Fraudulent activity in this context has significant consequences. Legitimate graduates find themselves competing unfairly against those with falsified credentials, resulting in disappointment and missed chances. Additionally, employers wrestle with the challenging task of confirming the legitimacy of candidates' educational histories, often resorting to lengthy and manual verification procedures. This problem not only undermines trust in the education system but also impedes economic progress and innovation. To address this urgent problem, we have embarked on a mission to harness the potential of blockchain technology. Blockchain, known for its decentralized and immutable nature, offers a promising solution to tackle the scourge of fake degree certificates. By recording and validating educational credentials on an incorruptible ledger, we aim to restore trust in the education system and empower both graduates and employers with a reliable means of verification. [11]

Our efforts are centered around the specific context of education in Bangladesh. The country has a variety of educational institutions that contribute to its progress. However, due to the absence of a reliable verification system, these institutions are vulnerable to fake degrees. According to data from the World Health Organization (WHO) as of January 10, 2022, nursing personnel in Bangladesh show a clear gender distribution. Around 90 percent are female professionals, while males make up only about 10 percent. This data highlights the gender dynamics in the nursing sector and the changing makeup of healthcare professionals in the country [9]. Our work aligns with the vision of digital transformation advocated by the Bangladesh government, as outlined in the ”Digital Bangladesh” initiative. As per the World Bank's report ”Higher Education in Bangladesh: Overcoming Challenges to Harness Opportunities” - World Bank, 2019 [10], the growth of the education sector in Bangladesh has been accompanied by challenges related to quality assurance and transparency. Our project draws inspiration from such findings and seeks to offer a tangible solution to the challenges posed by counterfeit degrees.

A. *Goal*

To investigate and recommend the use of blockchain technology as a secure and reliable method for validating academic certificates.

B. *Objective*

- Explore blockchain technology for secure certificate validation.
- Investigate the impact of blockchain on fraud prevention and certificate authenticity.
- Assess the benefits and challenges of implementing blockchain for businesses, educational institutions, and certificate holders.

The upcoming sections of the article are organized as follows: Section II furnishes an overview of the existing literature regarding the incorporation of blockchain for counterfeit certificate detection. In Section III, we elaborate on our proposed methodologies, data collection strategy, chosen methods, and analysis procedures. Section IV discusses the system's implementation, encompassing integration aspects and challenges encountered. Within Section V, we present the results and engage in a discussion regarding our system. In Section VI, we delineate our future work plans and provide a conclusive summary.

II. LITERATURE REVIEW

The article titled ”Academic Certificate Fraud Detection System Framework Using Blockchain Technology” by Lutfiani, Ninda, et al. (2022) proposes a framework for detecting academic certificate fraud using blockchain technology. The authors discuss the growing issue of fraudulent certificates in the academic sector and how blockchain can be utilized to address this problem. The paper presents a detailed overview of the proposed framework, which involves the use of blockchain for secure verification and storage of academic certificates. The authors also highlight the advantages and limitations of their framework. This article can be a valuable resource for researchers and practitioners interested in exploring the application of blockchain technology in combating academic certificate fraud. [1]

The paper focuses on employing blockchain for verifying academic certificates in higher education. Educational institutions must maintain student details from enrollment to degree completion, as certificates hold significant value in reflecting skills and knowledge. With 28% of discrepancies attributed to fake degree submissions and 27% to fake universities in 2020, fake academic certificates pose a significant issue. The study identifies five sources of counterfeits and introduces blockchain technology to enhance verification. The Blockchain for Education platform, initially utilized by the University of Nicosia, secures certificate access and management. SHA256 hash algorithm generates certificate hashes, verified by locating them within index documents. Infrastructure like Sovrin supports global digital identities, while Apostille serves notarization purposes. A proposed Hyperledger Fabric framework ensures secure network participation, transaction management, and confidentiality for academic certificates. Records Keeper employs blockchain to verify certificates, providing users with receipts for third-party validation. The study concludes by highlighting the transformative potential of blockchain in issuing, validating, and sharing certificates, along with presenting use cases and evaluation results. Overall, the paper underscores the role of blockchain in fortifying certificate authenticity and security within higher education. [2]

The main theme of the paper ”Blockchain Technology and Academic Certificate Authenticity—A Review” by Kumutha K. and Jayalakshmi S. revolves around the exploration and evaluation of how blockchain technology can enhance the authenticity of academic certificates. The paper undertakes a comprehensive review of the applications and implications of blockchain in the context of verifying the legitimacy of academic certificates. The goal of this project is to improve the document verification process by utilizing blockchain technology. Furthermore, the paper aims to broaden knowledge about blockchain by recognizing the benefits, risks, and difficulties associated with the effective execution of application-supported blockchain technology, aligned with principles and rules for educational certificate verification. The authors propose an academic certificate authentication system based on blockchain technology as a solution to mitigate the use of forged papers. Through this review, the authors provide insights into the potential of blockchain to revolutionize the way academic qualifications are validated and secured while addressing the challenges and opportunities that arise in its implementation. [3]

The important issue of fake certificates in Vietnam is addressed in the work ”Towards a blockchain-based certificate authentication system in Vietnam” by Nguyen, Binh Minh, Thanh-Chung Dao, and Ba-Lam Do, which was published in PeerJ Computer Science in 2020. In an effort to address the problem that is widespread in the nation, the authors suggest a blockchain-based system as a potential remedy to improve the authenticity and integrity of certificates. To do this, the authors take a pragmatic approach by creating and putting into use a blockchain system prototype that is specifically made for certificate authentication. They manage the authentication process using the Ethereum blockchain platform and smart contracts. The proposed approach secures the tamper-proof character of certificates and offers a visible and auditable authentication procedure through cryptography and decentralized consensus processes. The system consists of several processes, all of which are carried out utilizing blockchain technology, including certificate issues, verification, and revocation. The solution increases the reliability of certificates and reduces the dangers related to fake certificates by utilizing the immutability and transparency aspects of the blockchain. Through simulations and experiments, the authors assess the efficiency, scalability, and security of their blockchain-based system, showing its benefits over more conventional centralized methods. By demonstrating the potential of blockchain technology to enhance the dependability and authenticity of certificates in Vietnam and elsewhere, this research makes a contribution to the field of certificate authentication. [5]

The paper explores the potential of blockchain technology in addressing the pressing issue of counterfeit certificates, which pose risks to individuals and public safety. Through a literature review, the study proposes an innovative model for issuing and verifying blockchain certificates. Research by Johnson et al. (2018) highlights the widespread presence of fraudulent credentials, particularly in critical sectors like healthcare and engineering, adversely affecting deserving candidates. Blockchain's transparency, immutability, and decentralized nature offer an optimal framework for combating these challenges. The blockchain's tamperproof features and cryptographic techniques ensure secure data storage and verification. In the education sector, Smith et al. (2017) introduced a blockchain-based model tailored for verifying educational certificates. This decentralized network streamlines the secure issuance of digital certificates, fortified by digital signatures that enable convenient employer verification. However, challenges concerning privacy, scalability, and interoperability necessitate further investigation in future research endeavors. In essence, blockchain technology demonstrates considerable potential in ensuring secure certificate verification. The intended research aims to construct a model harnessing blockchain's distinct attributes to enhance trust, mitigate risks, and elevate the integrity of certificate-based systems. This research builds upon the foundation laid by studies like "Certificate Verification System using Blockchain" by Khandelwal et al. (2020), further contributing to the advancement of secure document verification processes. b4

III. METHODOLOGY

The provided diagram Fig. 1 illustrates a laborious and time-intensive manual verification process. Initially, candidates send their certificates to the organization, which subsequently forwards them to the respective candidates' universities for verification. The universities independently scrutinize the certificate copies and engage a third-party agency for further investigation. Following this, a comprehensive verification procedure takes place. If the certificates align with the originals, the university is informed. However, in cases of disparities, appropriate actions are taken against the candidates.

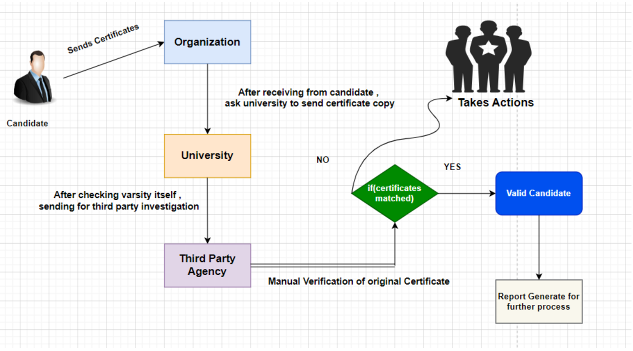

Sends Certificates
Organization
Candidate
After receiving from candidate , ask university to send certificate copy
Takes Actions
University
NO
YES
if(certificates matched)
Valid Candidate
After checking varsity itself , sending for third party investigation
Third Party Agency
Manual Verification of original Certificate
Report Generate for further process

Fig. 1. Manual verification process.

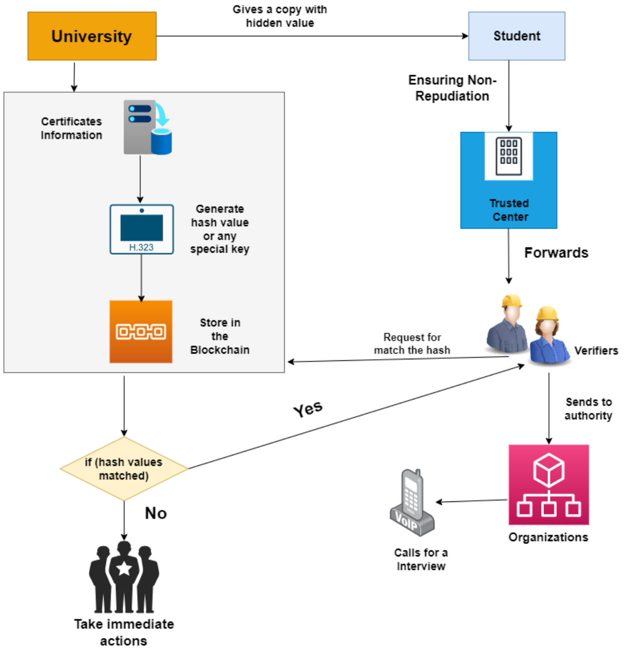


Fig. 2. Our proposed blockchain-based verification process.

To eliminate the manual process, we propose a blockchain-based methodology Fig. 2. In this approach, the university provides an original copy with a concealed value to the student, while another copy is sent to the blockchain. The blockchain securely stores candidates' information and generates a hash value or unique key, which is then stored within the blockchain. When students submit their certificates to verifiers, the process goes through a trusted center, ensuring a record of certificate submission. The trusted center then forwards the certificates to the verifiers. The verifier initiates a request to match the hash in the blockchain. If the hashed value aligns with the hidden value of the certificate, the verifier communicates the outcome to the organization for further steps. In cases where a discrepancy is detected, indicating a mismatch in values, appropriate actions are taken against the certificate holder. This blockchain-based approach ensures transparency, tamper resistance, and a streamlined verification process.

A. Data Collection Strategy

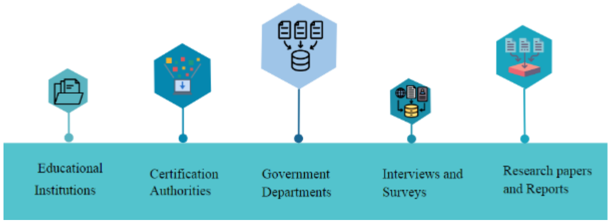


Fig. 3. Data collection strategy for our system.

To detect fake certificates, data will be collected from various sources mentioned in Fig. 3 including educational institutions, certification authorities, and government departments. Interviews and surveys will be conducted with officials to understand their processes and measures for preventing fake certificates. Discussions with employers, academic institutions, and job seekers will provide insights into challenges and red flags for detecting fake certificates. Secondary sources such as research papers and reports will be analyzed. Data analysis will identify patterns and trends associated with fake certificates. Based on the findings, a system for detecting fake certificates will be developed, incorporating machine learning algorithms and data validation techniques. The data collection strategy aims to gather information from stakeholders and real-life scenarios to ensure an effective and practical fake certificate detection system.

B. Data Collection Method

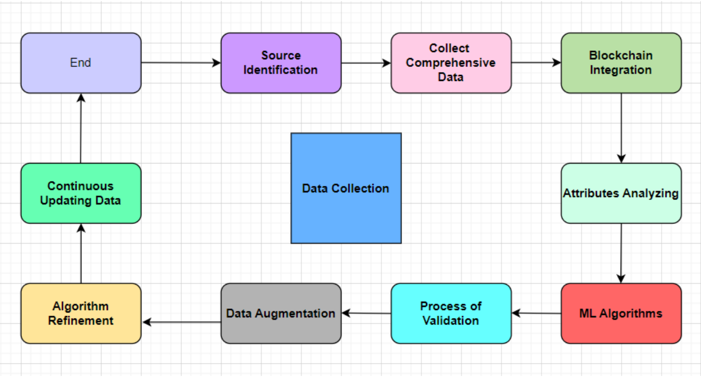


Fig. 4. Data collection method for our system.

The data collection method mentioned in Fig. 4 for detecting fake certificates using blockchain involves a fascinating process that combines advanced technology to reveal fraudulent certificates and ensure reliability. In the quest to uncover fake certificates, the first step is to identify relevant sources like educational institutions and certification authorities. Once these sources are pinpointed, a comprehensive dataset is diligently collected, encompassing both genuine certificates and those suspected to be fraudulent. This trove of data is then seamlessly integrated into a specialized blockchain system designed to validate and verify certificates. Now comes the intriguing part. Every attribute of the certificates, from issuer details to unique identifiers, is carefully captured, like pieces of a puzzle waiting to be solved. With the data in hand, powerful machine learning algorithms step onto the stage, sifting through the attributes, searching for patterns, and uncovering anomalies that indicate potential fake certificates. But the journey doesn't end there. The validation process takes center stage, leveraging the blockchain's decentralized and transparent nature. The certificates undergo scrutiny, ensuring that only legitimate ones pass the test, while any suspicious entries are meticulously flagged. To strengthen the detection capabilities, data augmentation techniques come into play, enriching the data set with external information sources. This broader perspective allows for a more comprehensive understanding of the intricate world of certificate fraud. The story continues as the detection algorithms are fine-tuned and refined based on the obtained results, aiming to enhance accuracy and effectiveness. Metrics like precision, recall, and accuracy become the guiding stars, illuminating the path toward a robust and reliable detection system. The saga of detecting fake certificates never ends, thanks to continuous data updating. New instances of suspected fraudulent certificates are seamlessly incorporated, keeping the system on its toes and always ready to adapt. In this captivating tale of data collection, blockchain technology unveils its power, empowering us to develop an unyielding system that safeguards the authenticity of certificates, ensuring trust and reliability.

C. Data Analysis

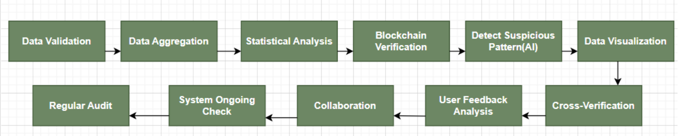


Fig. 5. Data analysis for our system.

In Fig. 5 we can see after collecting the data, we validate its completeness and accuracy. Then, we aggregate certificates based on specific criteria and perform statistical analysis to identify patterns and anomalies. Utilizing the blockchain, we verify the authenticity of certificates and employ machine learning algorithms to detect suspicious patterns using AI. Data visualization helps present insights effectively, while cross-verification ensures data accuracy through external sources. Gathering user feedback allows us to continuously improve the system's performance and collaborate with relevant authorities to share insights and combat fraudulent activities.

Implementing continuous monitoring and conducting regular audits for data protection and compliance ensures a robust and reliable system to safeguard against fake certificates over time.

IV. System Implementation

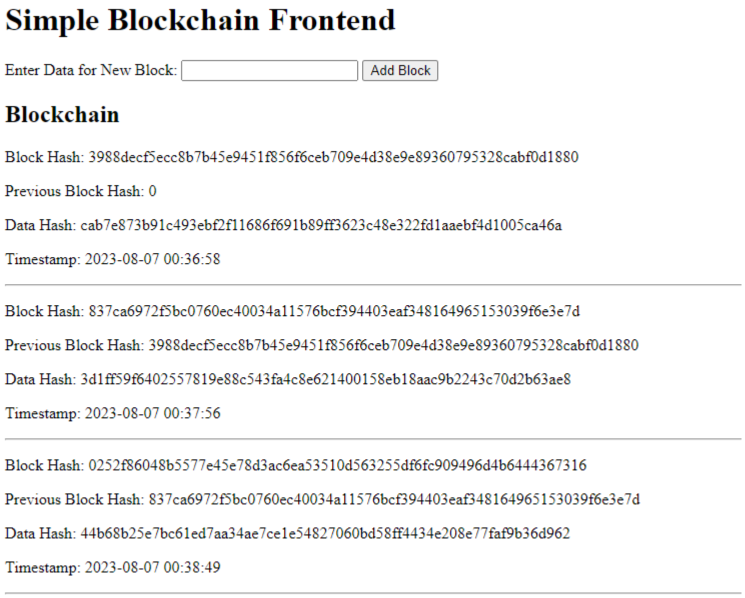
Our system, designed to tackle the problem of fake degree certificates, combines smart technology with robust security measures. We've developed a user-friendly web platform using PHP and MySQL, allowing educational institutions to record and validate certificates. The heart of our solution lies in blockchain technology, which acts as an unchangeable ledger to secure the authenticity of certificates. When a certificate is issued, it's digitally signed and stored on the blockchain, preventing any unauthorized changes. For verification, employers can use our intuitive interface, where certificates are instantly checked against the blockchain's records. The system integrates additional security tools like Hardware Security Modules for safeguarding cryptographic keys and secure communication protocols. This unified approach not only provides quick and reliable certificate validation but also ensures trust in academic qualifications, benefiting both graduates and employers while mitigating the risks associated with counterfeit degrees.

A. Integration and Challenges

Integrating our system involved merging multiple components seamlessly. We synchronized the blockchain with the database system, ensuring data consistency between the two layers. Challenges emerged in optimizing system performance while maintaining security. Coordinating the secure communication between blockchain nodes, web servers, and HSMs required careful design. Additionally, ensuring user-friendly interfaces across devices posed a usability challenge. Overcoming these hurdles demanded a collaborative effort between developers, security experts, and UI designers, resulting in a comprehensive system that merges technology with practicality.

V. Results and Discussion

In Fig. 6, our study shows that using blockchain technology can make certificate validation much stronger and more dependable. By using blockchain's special features that keep things secure and can't be changed, we made sure academic achievements are real and stopped fake certificates. Our research pointed out the good things about using blockchain to stop fake certificates. The transparency and unchangeable nature of blockchain records build trust and stop cheating. Also, using blockchain to verify certificates can save a lot of time and money for employers, schools, and people who have certificates. Using blockchain for certificates looks promising, but we need to deal with challenges like privacy, scalability, and compatibility. Our research adds to what we know about how blockchain could change certificate validation. By combining fancy technologies like machine learning and blockchain, we suggest a smart way to fight fake certificates. Switching to blockchain-based methods is a big change that can stop cheating and make certificates more trustworthy. This also helps students, schools, and employers. We found that using blockchain to validate certificates is a good idea to fight fake certificates. Mixing high-tech stuff with teamwork and careful watching can give us a safe solution that helps everyone involved in certificates. In the future, we should focus on solving the challenges we found and using blockchain, even more, to make certificates very reliable. As technology gets better, we might even reach a point where verifying certificates is 100% accurate. Our research shows that working together and coming up with new ideas can use blockchain to make certificates more reliable.



```
Blockchain

Block Hash: 3988decf5ecc8b7b45e9451f856f6ceb709e4d38e9e89360795328cabf0d1880
Previous Block Hash: 0
Data Hash: cab7e873b91c493ebf2f11686f691b89ff3623c48e322fd1aaebf4d1005ca46a
Timestamp: 2023-08-07 00:36:58

Block Hash: 837ca6972f5bc0760ec40034a11576bcf394403eaf348164965153039f6e3e7d
Previous Block Hash: 3988decf5ecc8b7b45e9451f856f6ceb709e4d38e9e89360795328cabf0d1880
Data Hash: 3d1ff59f6402557819e88c543fa4c8e621400158eb18aac9b2243c70d2b63ae8
Timestamp: 2023-08-07 00:37:56

Block Hash: 0252f86048b5577e45e78d3ac6ea53510d563255df6fc909496d4b6444367316
Previous Block Hash: 837ca6972f5bc0760ec40034a11576bcf394403eaf348164965153039f6e3e7d
Data Hash: 44b68b25e7bc61ed7aa34ae7ce1e54827060bd58ff4434e208e77faf9b36d962
Timestamp: 2023-08-07 00:38:49
```

Fig. 6. Hash value generated for each certificate.

VI. Conclusion and Future Study

Our research provides a strong foundation for blockchain's integration in certificate validation, yet future efforts can amplify its impact. Key focuses include enhancing privacy through techniques like zero-knowledge proofs, scaling blockchain architecture, and ensuring interoperability with legacy systems. Cross-border recognition and user-friendly interfaces should be explored for international adoption, while hybrid solutions incorporating AI and biometrics can heighten accuracy. Security measures and data archiving must persist, and cross-domain applications, such as professional certifications, warrant exploration. Real-world implementation and partnerships with educational institutions will validate the system's practicality. Tackling these areas will propel blockchain-based validation as a reliable solution against fake certificates, bolstering trust and integrity within academia. Embracing innovation and collaboration ensures a secure and seamless transition toward a trustworthy certification process.

Acknowledgment

We extend our heartfelt appreciation to our mentor, Mir Moynuddin Ahmed Shibly, for his unwavering guidance, expertise, and encouragement throughout the course of this research. His valuable insights and constructive feedback played a pivotal role in shaping the direction of our paper. We are truly grateful for his mentorship, which greatly enriched our understanding and contributed to the success of this work. Additionally, we would like to thank all individuals and institutions that supported us.

References

[1] Lutfiani, Ninda, et al. ”Academic Certificate Fraud Detection System Framework Using Blockchain Technology.” Blockchain Frontier Technology 1.2 (2022): 55-64.

[2] Al Harthy, Khoula, Fatma Al Shuhaimi, and Khalid Khalifa Juma Al Ismaily. ”The upcoming blockchain adoption in Higher-education: requirements and process.” 2019 4th MEC international conference on big data and smart city (ICBDSC). IEEE, 2019.

[3] Kumutha, K., Jayalakshmi, S. (2022). Blockchain Technology and Academic Certificate Authenticity—A Review. In: Jeena Jacob, I., Gonzalez-Longatt, F.M., Kolandapalayam Shanmugam, S., Izonin, I. (eds) Expert Clouds and Applications. Lecture Notes in Networks and Systems, vol. 209. Springer, Singapore. 16 July 2021.

[4] Khandelwal, Harshita, et al. ”Certificate verification system using blockchain.” Advances in Cybernetics, Cognition, and Machine Learning for Communication Technologies (2020): 251-257.

[5] Nguyen, Binh Minh, Thanh-Chung Dao, and Ba-Lam Do. ”Towards a blockchain-based certificate authentication system in Vietnam.” PeerJ Computer Science 6 (2020): e266.

[6] F. Rhodes. Blockchain certificates: a prototype implementation for digitising educational certificates. Journal of Chemical Physics, 55,(393): 298–305, 1971.

[7] Melo, Wilson S., et al. ”Using blockchains to implement distributed measuring systems.” IEEE Transactions on Instrumentation and Measurement 68.5 (2019): 1503-1514.

[8] Ubayasiri, Kasun. ”Framing statelessness and’belonging’: Rohingya refugees in Bangladesh’s the Daily Star newspaper.” Pacific Journalism Review 25.1/2 (2019): 260-276.

[9] Ali, Syukrina Alini Mat, et al. ”Hackman and Oldham’s job characteristics model to job satisfaction.” Procedia-Social and Behavioral Sciences 129 (2014): 46-52.

[10] Sarker, Md Fouad Hossain, et al. ”Use of e-learning at higher educational institutions in Bangladesh: Opportunities and challenges.” Journal of Applied Research in Higher Education 11.2 (2019): 210-223.

[11] Dongre, Jayesh G., Sonali M. Tikam, and Vasudha B. Gharat. ”Education degree fraud detection and student certificate verification using blockchain.” Int. J. Eng. Res. Technol 9 (2020): 300-303.

The source code for our model can be found here: click