Using Blockchain Technology for Credentialing Educational Certificates in Bangladesh

***Abstract*—The opportunities and the obstacles of using blockchain technology in case of the academic sector are explored in this research.While looking for jobs, students must provide evidence of their academic credentials and extracurricular achievements, which are essentially in the form of certificates. It is a persistent problem in Bangladesh for people to create and submit false academic credentials, hence making it more challenging for genuinely trained people to get work in a field for which they are qualified. Checking the authenticity of academic documents is absolutely necessary before any recruiting process. While the current procedure is unable to ensure the authenticity of certificates, utilizing blockchain technology to establish an electronic certificate creates a record that cannot be altered in any way and is tamper-proof at the same time. This makes it far more difficult for students to forge their academic credentials thus eliminating fraudulent activities.**

***Index Terms*—blockchain; certificate credentials; IPFS; fake certificates; tamper-proof; decentralized**

I. Introduction

In the conventional educational model, students are awarded a number of certificates at various points of their educational journey that prove their academic achievements.There is currently no centralized system in place for digitizing all these certificates or verifying their authenticity, also increasing the risk that they may be lost or damaged. It is extremely difficult to maintain or authenticate such a huge number of records, which might lead to an inconvenient situation where certificates might be forged [1]. Fake certificate producers and students who use them to advance in their careers have been growing in recent years in Bangladesh. For a small fee, one can skip the trouble of attending school completely and get a certificate that is almost indistinguishable from the authentic one obtained from an educational institution. It is hard to say how many people with fake certificates are actively seeking jobs, but it is likely a large number given that few companies bother to verify applicants' credentials. Anyone caught using a forged signature or seal on a legal document in Bangladesh is subject to a fine of up to BDT 20,000 or two years in prison, or both, per Section 470 of the Bangladesh Penal Code, 1860. While police regularly conduct operations against certificate forgeries, they occasionally have trouble distinguishing between real and fake certificates because students frequently make photocopies of original certificates at the same shops [2]. So, to prevent this we need a system that eliminates any chances of tampering with the data. Blockchain technology would be the most effective and efficient way of implementing this proposal. Part of the proposed algorithm is implemented using the public Blockchain technique, while part of it is applied with the private Blockchain method for restricted approval behavior. When a university or other institution uses Blockchain, that adds a block automatically to the other members of the network due to the network's decentralized nature [3].

II. Background

A. Blockchain and its types

A well known definition of the blockchain technology as stated by Don and Alex Tapscott is- "The blockchain is an incorruptible digital ledger of economic transaction that can be programmed to record no just financial transactions but virtually everything of value" [4]. This statement refers to the opportunities of blockchain technology in not only being in financial transactions but in various other non-financial fields where anything of value can be recorded without corrupting the data itself. To expand, a blockchain is a publicly distributed database that contains records of all conducted transactions or digital events and is accessible to shared groups. The majority of nodes in the network agree on the legitimacy of each transaction in the public ledger. Moreover, the data submitted to the system is permanent. Every transaction ever done is recorded in the blockchain and may be verified at any time [5]. There are four types of blockchain:

1) Public Blockchain: In this decentralized blockchain, anyone can access the network and based on the validation, the person who has been validated is given the transaction reward. Here, two types of consensus models are utilized- Proof-of-work (PoW) and Proof-of-Stake (PoS). Moreover, the public blockchain is non restrictive and permissionless.
2) Private blockchain: This blockchain network is private and restricted which works for closed systems and only selected members can join. Here, cryptocurrency is not required. Furthermore, this blockchain network runs with authorized nodes thus no one outside the organization has access to the information. This network is more efficient, the transactions are faster, more scalable and overall faster compared to public blockchain. However, it is weak against third party attacks as the management is centralized.
3) Hybrid Blockchain: In this blockchain, both public and private blockchains are merged. With benefits of both combined in one. This blockchain has enhanced security and transparency.

4) Consortium Blockchain: This blockchain is semi-decentralized which is mostly used in the organization of managing blockchain networks [6].

B. Properties of Blockchain

According to [7], there are several properties of blockchain that make it a suitable technology for a variety of applications. Firstly, Blockchain is decentralized, meaning that there is no central management making the system proof of a single point of failure. Secondly, it is transparent and traceable- meaning, the data is accessible to any person who is validated on the blockchain network. Moreover, blockchain is immutable. The immutability of blockchain refers to the fact that once data is entered into the blockchain, it is unchangeable thus gaining the trust of its participants [8].

III. Literature Review

Blockchain technology is a decentralized system serving as one of its primary advantages. In addition, blockchain technology can completely eliminate third party involvement and a central administrator [4]. According to [4], as each transaction is recorded and data is available to all participants, this results in Blockchain being immutable, traceable and trustworthy. Initially, Blockchain had been used solely as a peer-to-peer transaction system of electronic cash, where transactions between two parties, the sending and receiving, occur without any involvement of a third party financial organization [9]. However, as more time passes, Blockchain technology is evolving, thus, newer applications of the technology are being explored. As a growing field of interest, with its highly modern nature, Blockchain is suitable for application in many fields and one of the fields it can be of relevance to is education. This section reviews the usage of Blockchain in the education sector and educational certificate credentials using Blockchain Technology. Blockchain is a domain which is being explored constantly, thus the research regarding Blockchain's usability and application in the education sector is still fragmented and incomplete [10]. As a technology which has gained popularity due to its exceptional cyber security capabilities [11], its potential has been increasing gradually and has benefited the academic sector as well. According to Alammary et.al [12], Blockchain's application in education can be grouped into twelve categories which essentially are the following :Management of certificates, qualifications and learning outcomes management; assessment of students' professional potential; safeguarding of collaborative learning environments; transfer of fees and credits; obtaining consent from digital guardians; management of competitions; management of copyrights; enhancing student interactions in online learning; review of exams; and promotion of lifelong learning. It was also found by [12] that the vast majority of applications were devoted to managing certificates where 13 articles—or 41%—of the total—presented software tools for controlling the distribution, storage, and exchange of academic credentials for students. Tellew et.al [13] proposed a system, CertificateChain, where the training certificates for healthcare workers are to be managed using blockchain and smart contracts. In their proposed model, Ethereum was used where the certificates were stored in blocks after being split into 30KB slices due to transaction size limitations followed by their algorithm which reconstructed the file into a byte array on the chain. Another work by Reza el.at [14] suggested a system emphasizing on academic records authentication along with combining educational institutions with the intention of expanding the storage system using blockchain. By deeming digital certification as an importance alongside the rise of fraudulent certificates, Alam et.al [15] proposed a blockchain-based system for verifying academic credentials. In their system, the information of the student will be entered into the blockchain after undergoing hashing algorithms which will be included in a QR code of the eCertificate. The QR code will be included in the physical copy of the certificate for the verification procedure. Oliver et.al [16] in his research for using blockchain as a tool for tracking and verification of official degrees proposes a business model by using Blockcerts which is an open source platform by the Massachusetts Institution of Technology focusing on leveraging blockchain to issue and verify government certificates in the United Kingdom. In his work, Jayesh et.al [17], proposed a system where fraudulent educational certificates are to be detected and original certificates can be verified using blockchain. In their system, the students and employers both can register and apply for authentication, renewal and issuing of certificates where the certification data will be stored on blockchain which can be accessed by institutions, students and job recruiters. Hasan et.al [18] discussed a blockchain-based certificate verification system, DistB-CVS, from Bangladesh's perspective, where they laid out a detailed architecture for their system. To summarize, the scopes of blockchain technology's applications are wide even in fields of education. However, in contrast to other research works for using blockchain technology for credentialing educational certificates, our work focuses on the use of Interplanetary File System (IPFS) to store the certificates in an attempt to lower the transaction costs.

IV. Methodology

A. Creation of block and information storage

Educational institutions authorized on the blockchain server by the government would create blocks containing student information on the blockchain such as student's name, birth date, NID, student's grade point average at that institution along with other information such as timestamp, transaction ID and nonce upon the completion of the student's education. The genesis block for each student is created with their unique NID number and then when an institution has to store the student's digital certificate on the block, a new block with the information of the previous block's hash is created. After the creation of the block with all information, the block will be closed and considered tamper-proof. The block that follows will appoint a new hash with the hash value of another certificate of achievement with the CID value of the certificate fetched from IPFS.

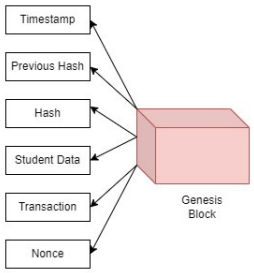

Fig. 1. Genesis Block of a Student

B. Underlying workings of the system

There are 2 types of users in our system: authorized educational institutions and general users which consist of students and private or public organizations which will serve as job recruiters. Here, we propose the usage of Hybrid blockchain, where the private blockchain belongs to the educational institutions which will maintain the privacy of the student's data and the public blockchain lets the general users access and view the data of the student, along with their certificates. The certificate will be stored on IPFS, where the hash value for the image will be stored in the block of the student. General users can access the digital certificate stored in IPFS with a public key and private key, which will be provided by the institution for accessing the respective student's information.

C. Certificate storage in Blockchain using IPFS

In our system, blockchain is merged with InterPlanetary File System (IPFS) to obtain a decentralized network as well as minimize transaction costs as a larger file size corresponds to higher cost. A single IPFS is capable of storing up to 256 KB of data [19]. And with files larger than 256 KB, the file can be broken down into smaller chunks by this distributed ledger. The smaller chunks are connected to form a larger file in an empty IPFS object [20]. However, to maintain the speed of accessibility, the file size is to be kept at 256 KB. The image of the digital certificate of the student provided by their institution is stored in IPFS. IPFS, as it uses content addressing which is identified by a cryptographic hash to identify the data's physical location for accessing, is more resistant to intrusion than other file storages. The hash value of the digital certificate generated will be stored on the blocks of the student for quick access of the file.

Figure 2 & 3 summarize the working of the system.

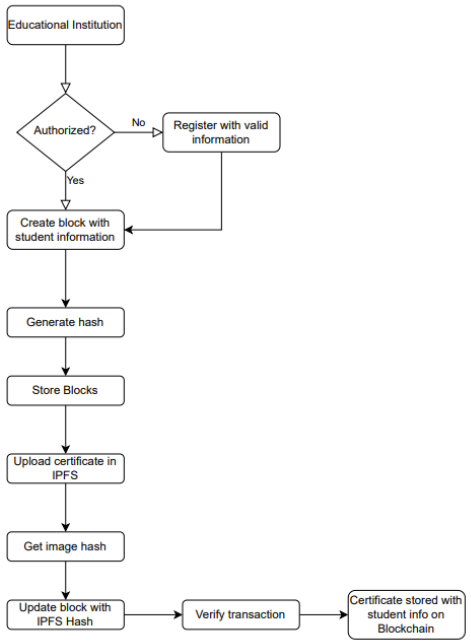

Fig. 2. Data flow of the student information and their credentials

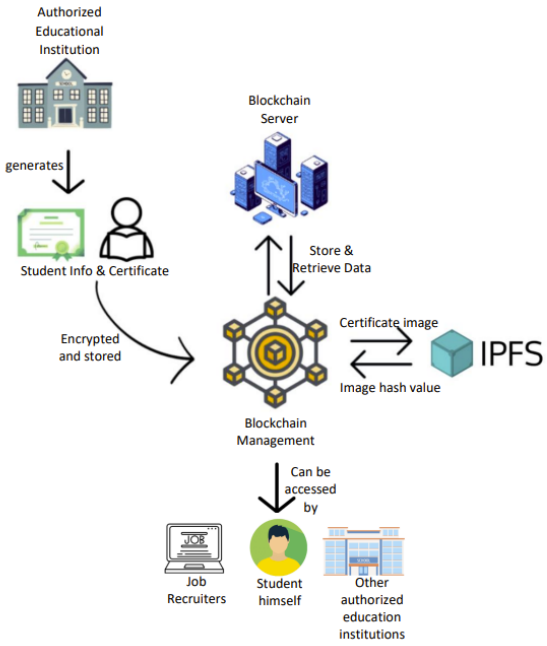

Fig. 3. Working Principle of the Certificate Storage and Viewing System using Blockchain

V. Analysis of Proposed Model

A. Benefits of our proposed system

Compared to traditional certification systems where the data may or may not be stored on a database, the authentication of certificates still remains an issue at hand. Hence, using blockchain technology to store digital certificates which will be updated on the network by authorized institutions will ensure the authenticity of the students credentials. Our system uses hybrid blockchain technology to store information, which makes the data decentralized, traceable and transparent as well as preserving the privacy of personal data of the students

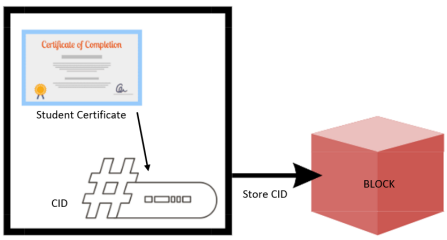

Fig. 4. Storing CID generated by IPFS to Blockchain

due to the presence of both permissioned and permissionless systems. Moreover, the use of IPFS for storing images along with blockchain ensures the decentralization of all data as IPFS itself is a distributed file system. Both data integrity and security is thus maintained using our system. Here, the students largely benefit from having a transparent view of their academic credentials and organizations which are potential employers of the students also benefit as they can be sure of the authenticity of the applicant's credentials.

B. Challenges and weaknesses of our system

The proposed technology is both safe and effective, but there are still certain obstacles to overcome. The present restriction on cryptocurrencies in Bangladesh has led many to believe that blockchain technology in general is also illegal [21]. It is difficult to apply blockchain technology on a broad scale because it is not yet widely adopted in Bangladesh. It's also possible that, at the present time, not everyone has access to the Internet or has the skills to use computers. Blockchain technology, however, has several uses outside of digital currencies and the financial sector. It can take a long time for businesses and schools to learn about blockchain's potential benefits and implement the technology. And then there's the issue of power usage. A country like Bangladesh with low energy resources can have environmental concerns due to the high energy consumption of blockchain networks. Scalability is a further significant obstacle. This is because the blockchain may become overloaded if too much information about students and their credentials is added at once. Furthermore, interoperability is a significant obstacle because protecting the system from outside intervention is currently difficult. As IPFS stores data in a decentralized fashion, hence "orphaned data" may pose a significant problem if the nodes storing the data go offline or the content is not popular, making it difficult to access or retrieve the credentials for education. Another issue is that authorized academic institutions may go out of business, making it difficult to get to the data they hold; this is something we'll address in the section below on addressing some of the system's drawbacks. Finally, the system's reliance on an always-on Internet connection is a serious flaw. Education credentials stored on IPFS and the blockchain require a reliable internet connection to access. This might be a major challenge in places where internet access is limited or unavailable.

C. Mitigating some of challenges of our system

Here, we outline some of the approaches that may be taken to address the primary threats to our system and its viability.

First, blockchain education and training programs and workshops to increase blockchain knowledge among students, teachers, and administration might be implemented to help alleviate the issue of slow adoption. The issue of internet dependence may be solved by investing in the required IT infrastructure, such as access to computers and the internet, especially in outlying locations, and working with telecom carriers to increase internet coverage.

Next, a consensus method with relatively energy-efficient, such as Proof-of-Stake (PoS) and Delegated Proof-of-Stake (DPoS), might be incorporated in the system to help with the problem of high energy consumption. [22] The next challenge is the potential for data to become orphaned as a result of IPFS usage; this could be addressed by implementing content pinning strategies to keep data available even if some nodes go down, and by providing incentives for users to host and maintain data on IPFS. The concept of pinning in IPFS is crucial because it instructs IPFS to always preserve an object [23].

Lastly, addressing the problem that arises from shutdown of authorized educational institutions on blockchain, information that can benefit from decentralization can be stored in the public component, while sensitive data might be maintained in the private one. Furthermore, we may empower students or people with more agency over their data by leveraging the hybrid blockchain's access control capabilities. They need the option to grant or withdraw access to their credentials and even sell or trade them. If we move non-sensitive data or verification-related information to the public portion of the blockchain, then crucial verification data will still be available and verifiable in the event that the private part of the blockchain is compromised due to the collapse of an organization. Moreover, it is important to define the steps to be taken while preserving data by data archiving, both in the public and commercial sectors, to guarantee that information from the past may be accessed for auditing and regulatory reasons.

VI. Conclusion

Blockchain and IPFS enhance the verification of academic degrees where blockchain saves certificate hashes for validation and IPFS digital storage decreases the chance of certificate loss. Future work could involve the Integration of several blockchain platforms and the enhancement of system capabilities. Another future work could involve the implementation of data deletion or redaction protocols in accordance with privacy regulations. Overall, this system has the potential to alter how academic certifications are validated and made reliable .The rising use of blockchain for certification implies that accessing academic credentials will become more efficient and safe in the future.This technology is perfect for securely storing,

sharing, and networking private information. This advanced tool can improve the efficiency, clarity, and quality of many existing systems. Credentialing, copyright protection, and instantaneous communication are all brought closer together by this method. Eventually, blockchain might improve these into more conventional methods.

REFERENCES

[1] N. V. Gopal and V. V. Prakash, "Survey on blockchain based digital certificate system," 2018. [Online]. Available: https://api.semanticscholar.org/CorpusID:221068010

[2] D. Tribune, "The fake certificate bazars of dhaka banginews.com," 2020. [Online]. Available: http://www.banginews.com/web-news?id=1e411713e3930fde89f48aed4dfb1608193b3fa5

[3] M. D. Pierro, "What is the blockchain?" *Computing in Science &amp Engineering*, vol. 19, no. 5, pp. 92–95, 2017. [Online]. Available: https://doi.org/10.1109/mcse.2017.3421554

[4] J. Golosova and A. Romanovs, "The advantages and disadvantages of the blockchain technology," in *2018 IEEE 6th Workshop on Advances in Information, Electronic and Electrical Engineering (AIEEE)*. IEEE, Nov. 2018. [Online]. Available: https://doi.org/10.1109/aieee.2018.8592253

[5] A. S. Kubeka, "P-v criticality of a modified BTZ black hole in 2 1 dimensional intrinsic time quantum gravity," *Journal of Modern Physics*, vol. 10, no. 03, pp. 294–301, 2019. [Online]. Available: https://doi.org/10.4236/jmp.2019.103020

[6] P. Paul, "Blockchain technology and its types—a short review," *International Journal of Applied Science and Engineering*, vol. 9, no. 2, Dec. 2021. [Online]. Available: https://doi.org/10.30954/2322-0465.2.2021.7

[7] K. Wust and A. Gervais, "Do you need a blockchain?" in *2018 Crypto Valley Conference on Blockchain Technology (CVCBT)*. IEEE, Jun. 2018. [Online]. Available: https://doi.org/10.1109/cvcbt.2018.00011

[8] F. Hofmann, S. Wurster, E. Ron, and M. Bohmecke-Schwafert, "The immutability concept of blockchains and benefits of early standardization," in *2017 ITU Kaleidoscope: Challenges for a Data-Driven Society (ITU K)*. IEEE, Nov. 2017. [Online]. Available: https://doi.org/10.23919/itu-wt.2017.8247004

[9] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," *Decentralized business review*, 2008.

[10] M.-F. Steiu, "Blockchain in education: Opportunities, applications, and challenges," *First Monday*, Aug. 2020. [Online]. Available: https://doi.org/10.5210/fm.v25i9.10654

[11] C. Atienza-Mendez and D. G. Bayyou, "Blockchain technology applications in education," vol. Volume 6, pp. 68–74, 12 2019.

[12] A. Alammary, S. Alhazmi, M. Almasri, and S. Gillani, "Blockchain-based applications in education: A systematic review," *Applied Sciences*, vol. 9, no. 12, p. 2400, Jun. 2019. [Online]. Available: https://doi.org/10.3390/app9122400

[13] J. Tellew and T.-T. Kuo, "CertificateChain: decentralized healthcare training certificate management system using blockchain and smart contracts," *JAMIA Open*, vol. 5, no. 1, Jan. 2022. [Online]. Available: https://doi.org/10.1093/jamiaopen/ooac019

[14] "Education certification and verified documents sharing system by blockchain," *International Journal of Intelligent Engineering and Systems*, vol. 15, no. 6, pp. 682–691, Dec. 2022. [Online]. Available: https://doi.org/10.22266/ijies2022.1231.60

[15] S. Alam, H. Abdullah, R. Abdulhaq, and A. Hayawi, "A blockchain-based framework for secure educational credentials," *Turkish Journal of Computer and Mathematics Education (TURCOMAT)*, vol. 12, pp. 5157–5167, 04 2021.

[16] T. A. Oliveira, M. Oliver, and H. Ramalhinho, "Challenges for Connecting Citizens and Smart Cities: ICT, E-Governance and Blockchain," *Sustainability*, vol. 12, no. 7, pp. 1–21, April 2020. [Online]. Available: https://ideas.repec.org/a/gam/jsusta/v12y2020i7p2926-d342271.html

[17] J. G. D. and, "Education degree fraud detection and student certificate verification using blockchain," *International Journal of Engineering Research and*, vol. V9, no. 07, Jul. 2020. [Online]. Available: https://doi.org/10.17577/ijertv9is070156

[18] M. Hasan, A. Rahman, and M. J. Islam, "DistB-CVS: A distributed secure blockchain based online certificate verification system from bangladesh perspective," in *2020 2nd International Conference on Advanced Information and Communication Technology (ICAICT)*. IEEE, Nov. 2020. [Online]. Available: https://doi.org/10.1109/icaict51780.2020.9333523

[19] S. Kumar, A. K. Bharti, and R. Amin, "Decentralized secure storage of medical records using blockchain and scpIPFS/scp : A comparative analysis with future directions," *Security and Privacy*, vol. 4, no. 5, Apr. 2021. [Online]. Available: https://doi.org/10.1002/spy2.162

[20] F. Liu, C.-y. Yang, Y. Jie, D.-l. Kong, A.-m. Zhou, J. Qi, and Z.-b. Li, "A hybrid with distributed pooling blockchain protocol for image storage," *Scientific Reports*, vol. 12, p. 3457, 03 2022.

[21] F. Zeya and S. Majumder, "Experts'perception on cryptocurrency trade in bangladesh: Fintech innovation or dilemma," *AN APPROACH TOWARDS CENTRAL BANK DIGITAL CURRENCY*, p. 300, 2022.

[22] L. M. Bach, B. Mihaljevic, and M. Zagar, "Comparative analysis of blockchain consensus algorithms," pp. 1545–1550, 2018.

[23] M. Kulüke, S. Kindermann, T. Kölling, and D. Klimarechenzentrum, "Ipfs pinning service for open climate research data," Copernicus Meetings, Tech. Rep., 2023.