2022 10th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO)
Amity University, Noida, India. Oct 13-14, 2022

2022 10th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO) | 978-1-6654-7433-7/22/$31.00 ©2022 IEEE | DOI: 10.1109/ICRITO56286.2022.9964545

Blockchain Technology in Digital Certificate Authentication

Adeeba Habeeb
Student, Information Technology Amity University Dubai,
UAE
adeebaH@amitydubai.ae

Vinod Kumar Shukla
Department of Engineering and Architecture Amity University Dubai,
UAE
vinodkumarshukla@gmail.com

Suchi Dubey
Manipal Academy of Higher Education, Dubai campus
United Arab Emirates
suchi.dubey@manipaldubai.com

Shaista Anwar
Khawarizmi International College, Abu Dhabi
United Arab Emirates
shaista.anwar@khawarizmi.com

***Abstract*: The paper presents the concept of the association of digital signature technology with the currently trending blockchain technology for providing a mechanism which would detect any dubious data and store it in a place where it could be secure for the long term. The features of blockchain technology perfectly complement the requirements of the educational fields of today's world. The growing trend of digital certificate usage makes it easier for a dubious certificate to existing, among the others hampering the integrity of professional life. Association of hash key and a time stamp with a digital document would ensure that a third person does not corrupt the following certificate. The blockchain ensures that after verification, nobody else misuses the data uploaded and keeps it safe for a long time. The information from the blockchain can be retrieved at any moment by the user using the unique id associated with every user.**

Keyword(s): Blockchain Technology (BTC), Education, E-Certificate, Digital Signature, Hash key

I. INTRODUCTION

The digitalization of almost every sector in today's period brought the challenge of requiring a system that securely records the transactions taking place and anything valuable. Such requirement led to the development of something known as blockchain technology (also known as distributed ledger technology) back in 2008 by Santoshi Nakamoto, intending to provide a technology that distributed the recorded data and made it impossible for editing or tampering. Blockchain technology is basically comprised of the following features [1].

1. Decentralizing of the data in terms of storage and maintenance over a distributed system. Adoption of a connection between nodes(blocks) through mathematical logic rather than a centralized way
2. Traceability states how two adjacent blocks are connected through a hash function, making every transaction accessible via a hash key, providing that the transactions are stored in a particular order of retrieval.
3. Immutability since any form of tampering would result in a change of the hash values, which would immediately be detected by the other nodes connected.
4. Currency properties since cryptocurrencies are inseparable from blockchain technology. Allows point-to-point transactions to take place without the involvement of any third party.
5. An anonymous transaction occurs as the security algorithms hash any data before sharing it.

Thus, it opens up a pool of opportunities for revolutionizing many social and economic groups like commerce, the industry, and the educational sector due to its efficiency in managing large amounts of data and providing a global transactional system. Blockchain technology majorly runs on a peer-to-peer network. It ensures that a set of protocols/instructions are obeyed by every participating node in the particular BCT, making it very reliable, trustworthy, secure and efficient. [2]

Blockchain technology is used in many domains due to its security features. Integration of blockchain technology can easily be seen in the finance-related domain [3] [4], in supply chain management [5], travel and tourism domain [6] and many related domains.

Many entities play a major role in the educational sector, including teachers, students, institutions, affiliation bodies, accreditors, etc. Implementing BCT in the education sector would result in a change in storing, managing and verifying a student's qualifications. Document verification is a tedious process, establishing a ledger which would track the progress and learning outcomes of a particular course due to which many educational institutes like schools, universities and colleges are applying to their campuses. The implementation of blockchain technology in the education sector could bring about a revolutionizing change both directly and indirectly. In the immediate context, it includes storing the student's qualification certificate or achievement information. In the informal context, information regarding the research skills, experience in workshops, internships, talents, and interests could be included.

With the numerous amounts of dubious degrees and educational qualifications being created and sold quickly, deploying the blockchain technology in identifying and managing student details serves as a mechanism that would filter out doubtful and fraud degrees, hence bringing out the number of such fraud cases. The fraud degrees could be easily spotted by matching the records with data stored with the student's id in the blockchain, which is then checked and verified by the miners (people responsible for maintaining the blockchain) from various places all over the globe. Being a highly efficient and reliable mechanism, its significance is trustworthy and immutable in identifying fraudsters [7].

978-1-6654-7433-7/22/$31.00 ©2022 IEEE

Among the first educational institutes to implement blockchain technology were the University of Nicosia and Sony Global Education, which utilized the BCT to generate a platform which would provide global assessment in storing and managing the degree information of students. Similarly, the Massachusetts Institute of Technology successfully created a digital badge whose core relies on blockchain technology for the online mode of learning. Whenever a student had completed attending the lab sessions of MIT lab media and passed an assessment based on it, it would automatically generate a certificate based on the same and store it into the blockchain network to avoid any manipulations/alterations in the information. It was in 2017 that the Holberton school adopted the blockchain technology in maintaining a BCT ledger that would store information regarding the degrees of students; the striking difference here was that they were the first educational institute that allowed the information in the ledger to be shared with the outside world [8]. A unique user ID was used to retrieve all information associated with an individual, including academic and non-academic excellence, research or project experience, and educational background of that particular individual [9].

Thus, such an implementation paved the way for all the educational institutes that provide bachelor's and master's degrees around the globe to create a similar ledger using blockchain technology for all the job aspirants of the world. By using a unique ID for each one of them, making the process of authentication of a degree and educational background information easily available to authorities places anywhere around the globe.

II. THE BLOCKCHAIN STRUCTURE

Any block taking part in a blockchain has 5 major components [10]

- ***MAIN DATA***- The data that is stored is mainly dependent of the kind of blockchain and transactions that take place in it between two nodes.
- ***HASH OF PREVIOUS BLOCK-*** A hash is generated when the transaction is initiated and then sent to the network
- ***HASH OF CURRENT BLOCK***- The block header records the last value of the hash
- ***TIMESTAMP***- Shows the time of the block creation
- ***OTHER INFORMATION***- Includes the signature of the block

III. DIGITAL CERTIFICATE

Certificates are essential documents which play an integral role in a person's professional life. There it's of prime importance that these records are stored in a tamper-proof manner and for long terms.

The digital certificate is one such document that presents the necessary data in the soft copy format. The basic idea is that a certificate/document is generated using an automated system that follows various secure algorithms. In this work, we will look at how blockchain technology could be used to store an E-certificate related to educational purposes. Since these certificates are issued by trusted third-party members or the certification authority, it resolves major security risks and authentication problems. This creates encrypted and secure online communication in the educational environment [11].

IV. SECURITY REQUIREMENTS FOR EDUCATIONAL E-CERTIFICATES IN BLOCKCHAIN

The e-certificates generated by any educational institution must fulfill some key security themes namely [12]**:** -

- ***AUTHENTICATION***- An authentication mechanism is mandatory with respect to every user that is a part of the system so as to uniquely identify them. This could be students/faculties.
- ***OWNERSHIP***- The recipient whose certificate in located in the block chain ledger has full authority/ownership over it.
- ***CONFIDENTIALITY***- This means to maintain the privacy of the information related to the student

V. BLOCKCHAIN TECHNOLOGY IN EDUCATIONAL ENVIRONMENT

There are three broad categories of the block chain technology

- Public blockchain
- Consortium blockchain
- Private blockchain

Each of these has its own distinct features like [13] [14].

- Public BT- allows each participant node to review and verify the transactions taking place. A known example to this is the Bitcoin
- Consortium BT- it assigns the authority in dealing with the transactions in advance. Ex- Hyperledger
- Private BT – the nodes have to follow certain restrictions to the access any data.

As discussed earlier, the specific requirements of an educational institute in terms of its security, the best-suited blockchain technology would be the Hyperledger technology or the consortium blockchain technology. The reason for a choice is that Hyperledger provides an access mechanism based on roles (in a sense, the authority of dealing with a given action is assigned rather than any node randomly dealing with it) [15].

Some of the benefits of using Hyperledger are [16] [17]

- A lesser complex alternative to developing a blockchain technology
- The access levels vary as per the requirements since it’s a role-based technology
- It’s a private blockchain since the records aren't really present in the public domain
- Access to the document is restricted by a time limit and can be viewed only on demand**.**

VI. ACADEMIC CERTIFICATES AND FORGERY

The forgery of academic credentials happens through counterfeiting and the meticulous involvement of various employees and institutions. Such an issue exists due to the lack of a robust mechanism that could be trustworthy enough to filter such dubious documents. Most academic institutions rely on the rustic process of verifications, which occasionally provide internal information without knowing to whom the information goes [18].

An example of an internal fraud that takes place quickly is; applying for an academic certificate without successfully graduating

Looking at the situation, it is pretty evident that a concrete mechanism is required to solve the issues of the certificate verifications, which would put a full stop to the frauds and offer better transparency. The main goal of this project is to achieve this through blockchain technology which would prevent any tampering, and digital signature technology that would allow the user to upload and share the respective document with the concerned authorities [19].

VII. PROPOSED SYSTEM ARCHITECHTURE

The process of verifications of educational documents is exceptionally tedious, considering there are thousands of job applicants floating around. The proposed system is a portal that allows uploading the certificates using the digital signature technology along with a blockchain which would safely store the data for long-term use, preventing tampering [20].

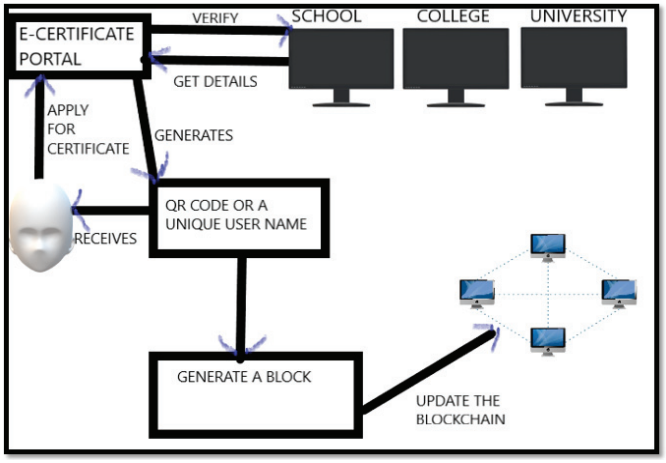

Fig 1. Process of Certificate authentication

The process begins with a newly graduated student looking for job opportunities/internships to apply into a web portal which would authenticate and generate an e-certificate (Fig 1). The web portal or the third party authenticates the appeal of an e-certificate by contacting the necessary school, college, or university. Upon verification, the blockchain generated for storing educational information of many students is updated, and the student is returned with a unique code or a QR code for any future document referral [21].

The received code can be submitted to any organization instead of a printed copy, which the company enters into the respective portal and can verify the authenticity.

VIII. PROPOSED SYSTEM AND DIGITAL SIGNATURE

To begin with, let's look into what digital signature technology is. The closest association of a digital signature could be a fingerprint; just as a fingerprint is unique to every individual, the digital signature is unique to every document signer (the one who uploads it). In technical terms, a digital signature is a coded message that links the signer with the document or uniquely identifies the signer [22]. Two keys are generated at the moment whenever the signer decides to sign a document [23] electronically.

Private key-

- Kept by the signer securely.
- Can be called as the hash of the document since it encrypts the data.
- The resulted encrypted data is what a digital signature is.
- A timestamp is added at the moment of creating a digital signature.
- Any minor change in the digital signature changes the hash value.

Public key-

- Holds the same value as the private key.
- Main difference is that is available to be shared publicly to verify the signed document.
- Any changes in the digital signature would not reflect in the public key.

The following illustration (Fig 2) shows how the verification is done.

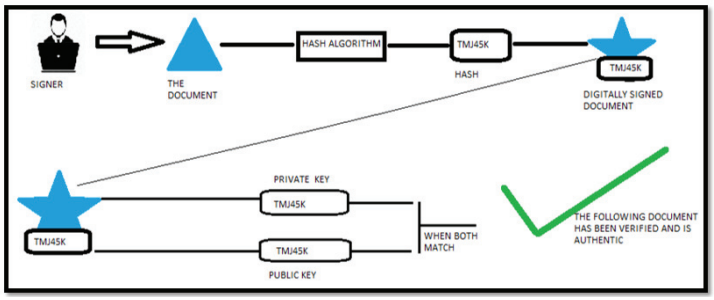

Fig 2. Verification process of Digital certificate.

If the original document were edited intentionally or unintentionally, the hash value would change from "TMJ45K" to a newer value. When anyone would enter the public key "TMJ45K," it would show an error as the document it was initially referring to no more has the same hash value [24] [25]. Fig 3 presents the flow of verification of digital certificates.

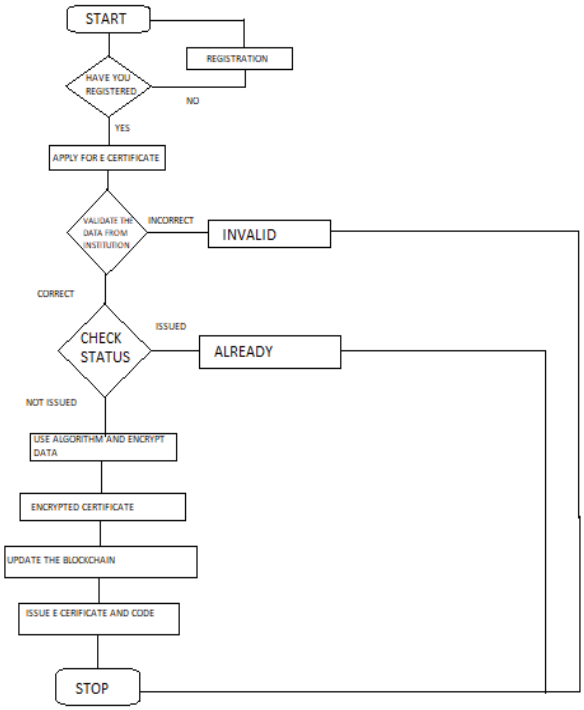

Fig 3. Flow chart for the verification of Digital Certificate

IX. HOW DOES THE BLOCKCHAIN TECHNOLOGY PLAY A ROLE IN THE PROPOSED SYSTEM

Every time the blockchain is updated with a new entry a block representing the given new data is generated as well like the following (Fig 4).

Fig 4. Hash Block component after each update

The three main components of a block are: -

1. ***Data***- Holds information as per the blockchain
2. ***Hash***- Uniquely identifies
3. ***Hash of previous block***- This is what actually creates a chain of blocks in a system

Blockchain helps prevent tampering with the stored data, as presented in Fig 5A and Fig 5B. If any tampering is done in the block, then the generated block will have a different hash and will not match the previous block, and this technique will prevent the tampering of the block.

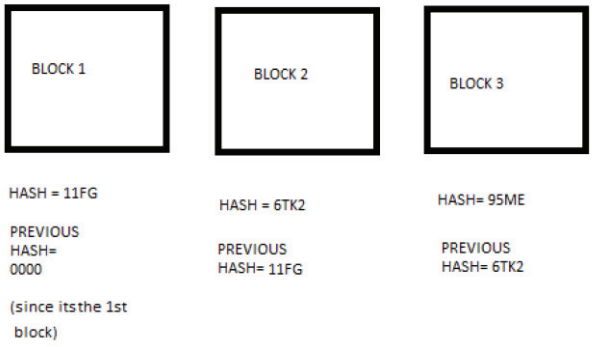

Fig 5A. Preventing technique of Blocks

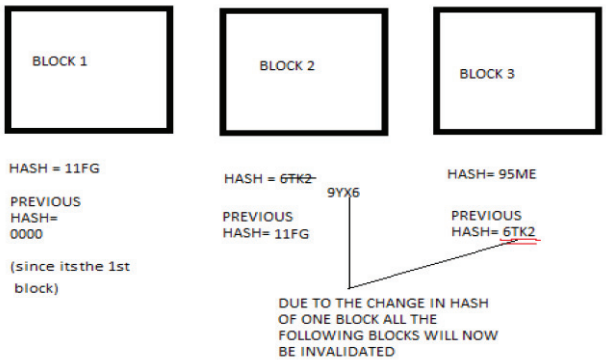

Fig 5B. Preventing technique of Blocks

X. CONCLUSION

The realization of the security and privacy requirements f the 21st century can be fulfilled by blockchain technology, which guarantees the protection of valuable properties and information then ensured by covering up the real identities of individuals by presenting the documents associated with them by unique id numbers. It provides equal access rights to the members and network associated with it. The association of digital signature technology with the blockchain perfectly forms a combination that would provide a reliable way of keeping the authenticity of the digital certificates ensuring the integrity of the educational environment. The biggest challenge ahead is a unified application of the same worldwide making it easier for educational services all around the globe.

REFERENCES

[1] Vyas, S., Shukla, V.K., Gupta, S., & Prasad, A. (2022). Blockchain Technology: Exploring Opportunities, Challenges, and Applications (1st ed.). CRC Press. https://doi.org/10.1201/9781003138082

[2] Chen, G., Xu, B., Lu, M., & Chen, N. S. Exploring blockchain technology and its potential applications for education. Smart Learn. Environ. 5, 1 (2018).

[3] R. Gupta, V. K. Shukla, S. S. Rao, S. Anwar, P. Sharma and R. Bathla, "Enhancing Privacy through “Smart Contract” using Blockchain-based Dynamic Access Control," 2020 International Conference on Computation, Automation and Knowledge Management (ICCAKM), 2020, pp. 338-343, doi: 10.1109/ICCAKM46823.2020.9051521.

[4] S. Anwar, V. K. Shukla, S. S. Rao, B. K. Sharma and P. Sharma, "Framework for Financial Auditing Process Through Blockchain Technology, using Identity Based Cryptography," 2019 Sixth HCT Information Technology Trends (ITT), 2019, pp. 099-103, doi: 10.1109/ITT48889.2019.9075120.

[5] L. Wanganoo, B. Prasad Panda, R. Tripathi and V. Kumar Shukla, "Harnessing Smart Integration: Blockchain-Enabled B2C Reverse Supply Chain," 2021 International Conference on Computational Intelligence and Knowledge Economy (ICCIKE), 2021, pp. 261-266, doi: 10.1109/ICCIKE51210.2021.9410677.

[6] Dubey, S., Subramanian, G., Shukla, V., Dwivedi, A., Puri, K., & Kamath, S. S. (2022). Blockchain technology: a solution to address the challenges faced by the international travellers. *OPSEARCH*, 1-18.

[7] Bond, F., Amati, F., & Blousson, G. (2015). Blockchain, academic verification use case. *Buenos Aires*.

[8] Albeanu, G. (2017, October). Blockchain technology and education. In *The 12th International Conference on Virtual Learning ICVL* (pp. 271-275).

[9] Kuvshinov, K., Nikiforov, I., Mostovoy, J., Mukhutdinov, D., Andreev, K., & Podtelkin, V. (2018). Disciplina: Blockchain for education. *Yellow Paper. URL: https://disciplina. io/yellowpaper. pdf*.

[10] Grech, A., & Camilleri, A. F. (2017). *Blockchain in education*. Luxembourg: Publications Office of the European Union.

[11] Nguyen, T. (2018). Gradubique: An academic transcript database using blockchain architecture.

[12] Hallak, J., & Poisson, M. (2007). *Corrupt schools, corrupt universities: What can be done?*. Paris: International Institute for Education Planning.

[13] Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. *Decentralized Business Review*, 21260.

[14] Lin, I. C., & Liao, T. C. (2017). A survey of blockchain security issues and challenges. *Int. J. Netw. Secur.*, *19*(5), 653-659.

[15] Aggarwal, S., & Kumar, N. (2021). Hyperledger. In *Advances in computers* (Vol. 121, pp. 323-343). Elsevier.

[16] Dinh, T. T. A., Liu, R., Zhang, M., Chen, G., Ooi, B. C., & Wang, J. (2018). Untangling blockchain: A data processing view of blockchain systems. *IEEE transactions on knowledge and data engineering*, *30*(7), 1366-1385.

[17] Plant, L. (2017). Implications of open source blockchain for increasing efficiency and transparency of the digital content supply chain in the australian telecommunications and media industry. *Journal of Telecommunications and the Digital Economy*, *5*(3), 15-29.

[18] Mahamat, M., Nigeria, A. N., YUSUF, S. I., Nigeria, A., & Kyrgyzstan, B. (2016). A Web Service Based Database access for Nigerian Universities' Certificate Verification System.

[19] Osman, G., & Omar, S. S. (2016). Cloud-Based Graduation Certificate Verification Model. In *Proceedings of Academics World 54th International Conference, Malacca, Malaysia* (pp. 571-14861269431620).

[20] Chen-Wilson, L., & Argles, D. (2010, January). Towards a framework of a secure e-Qualification certificate system. In *2010 Second International Conference on Computer Modeling and Simulation* (Vol. 1, pp. 493-500). IEEE.

[21] Cheng, J. C., Lee, N. Y., Chi, C., & Chen, Y. H. (2018, April). Blockchain and smart contract for digital certificate. In *2018 IEEE international conference on applied system invention (ICASI)* (pp. 1046-1051). IEEE.

[22] Wang, H., & Song, Y. (2018). Secure cloud-based EHR system using attribute-based cryptosystem and blockchain. *Journal of medical systems*, *42*(8), 1-9.

[23] Michalevsky, Y., & Joye, M. (2018, September). Decentralized policy-hiding ABE with receiver privacy. In *European Symposium on Research in Computer Security* (pp. 548-567). Springer, Cham.

[24] Wu, A., Zheng, D., Zhang, Y., & Yang, M. (2018). Hidden policy attribute-based data sharing with direct revocation and keyword search in cloud computing. *Sensors*, *18*(7), 2158.

[25] Khan, S., & Khan, R. (2018). Multiple authorities attribute-based verification mechanism for Blockchain mircogrid transactions. *Energies*, *11*(5), 1154.