Proceedings of the Second International Conference on Electronics and Sustainable Communication Systems (ICESC-2021)
IEEE Xplore Part Number: CFP21V66-ART; ISBN: 978-1-6654-2867-5

Blockchain based Framework for Student Identity and Educational Certificate Verification

Aastha Chowdhary, Shubham Agrawal and Dr. Bhawana Rudra
Department of Information Technology
National Institute of Technology Karnataka, Surathkal
Surathkal, India
aasthac67@gmail.com, shubham050300@gmail.com, bhawanarudra7@gmail.com

2021 Second International Conference on Electronics and Sustainable Communication Systems (ICESC) | 978-1-6654-2867-5/21/$31.00 ©2021 IEEE | DOI: 10.1109/ICESC51422.2021.9532968

***Abstract*— With the rise in digitization of documents stored online, it is important to have a document verification process. It involves customized verification and authentication of a document based on the content of the document. Among all the certificates, the educational certificate is one of the most important certificates, especially for students. Unfortunately, it is very easy to fake documents that are hard to identify nowadays and are often considered original. Blockchain has recently emerged as a potential alternative to manual verification of certificates. It provides a distributed ledger that is verifiable with cryptographic mechanisms. Also, it provides a common platform for easily sharing, storing, and accessing documents. The identity of the students can be verified using government authorized identity proofs. This paper proposes the use of such unique identity number and secret phrase provided by the student to further improve the security of the certificate verification system. The student's identity and document are both verified by matching the hashes already present in the Blockchain. Also, in the proposed method the documents are linked to the student to add another layer of verification. The implementation of this proposed platform can be used to issue, receive and verify the certificates.**

Keywords—Authentication, Blockchain, Cryptography, Educational Certificate Verification, Identity Proof, Secret Phrase

I. INTRODUCTION

Academic/Educational certificates serve as an indicator of human capital, including skills, competencies, aptitude, and knowledge. These certificates or qualifications are important mainly for employment as they serve as a guarantee for the candidate's skills and expertise, which shows their abilities and knowledge. The better the educational attainment levels, better the employment opportunities. As these certificates are extremely valuable, people often tend to lie about their academic qualifications by producing fake certificates.

An academic certificate is genuine when issued by a legally authorized university that is allowed to award such certificates. The fake academic certificates are generated from five different sources which include Fabricated Documents, Degree Mills, Modified Documents, In-House Produced, and Transactions [1]. As the fake documents precisely look like the originals, it is cumbersome for a layman to differentiate between the real and duplicate document. This issue of fake certificates has led to serious problems and these are generated in alarming proportions and need to be urgently tackled.

Blockchain technologies are recently introduced to improve the document verification process and to combat document frauds. Blockchain technology is a distributed database that combines many technologies such as cryptocurrency, algorithms, mathematics and distributed consensus algorithms. The blockchain comprises of six key elements: Decentralization, Transparency, Anonymity, Consensus Algorithm, Immutability and Open Source [2]. Blockchain technology can be used as an alternative solution for educational certificate verification and has recently emerged. It is used for educational certificate verification because it eliminates third parties which reduce the cost, documents are securely placed that only authorized people can access using their private keys, data is unalterable, etc.

Also, it is important to verify the student along with the certificate. This can be done by asking the user for his/her identity proof documents. However, the identity documents are generally in physical form and can be lost or stolen. If the identity documents are stored in a centralized server, they can be hacked and misused also. Therefore, in this work, we propose the use of biometric like a fingerprint, iris scanning or a unique identification number and a secret phrase that the student provides for additional security. These are combined and its hash is computed and stored on the blockchain.

Now to verify the certificates and the student, the hash of the student's unique number and secret phrase is checked for its existence in the blockchain. If a match is found, it implies that the student is a verified user. Then the hash of the student's certificate can be computed and compared to the hashes present in the blockchain. Again, if a match is found, it means the certificate is authentic. The major contributions of this research are as follows:

1) Implemented the Educational Certificate Verification using Ethereum blockchain and also verified the student's identity using this system.

2) Made the existing system more secure and robust by using unique identity number and unique secret phrase.

Authorized licensed use limited to: UT campus at Belfort Montebellard. Downloaded on August 10,2022 at 11:57:30 UTC from IEEE Xplore. Restrictions apply.

3) Linked certificate hash to the students as another layer of security to ensure that the issued certificate actually belongs to the student.

The rest of the paper is organized as follows. In Section 2, the relevant work in the field of Educational Certificate Verification is discussed. Section 3 explains the Proposed Framework adopted to solve the problem. Section 4 discussed the Implementation procedure and results which is followed by the Conclusion of this research work.

II. Literature Survey

Educational Certificates are an important indication of skill and are required to be submitted as proof while applying for higher education or a job. Due to such importance of these certificates, there have been several instances where fake documents have been discovered [3]. To overcome this issue, many techniques such as stamps, holograms and wet-signatures have been used [4], [5] but these are easily mimicable and can be replicated to create documents that are forged.

There are various existing research works and implementations of blockchain technology in different domains which have been proved to be more secure and reliable [6][20]. Blockchain acts as a common platform to share and store the data and access documents that decrease the overall time to verify certificates [16]. For storing user identity, a distributed application was implemented to integrate national identity numbers with blockchain so that a person need not carry the actual physical ID cards everywhere [7].

In [8], the application requires the participation of users which can be verified with the help of Blockchain. The user's government identity and biometric can be stored in a blockchain. Whenever a user's ID is accessed, a transaction is created for record purposes. Integrating both biometric and blockchain enhances the security of the whole system [9].

To verify the educational certificates, employers need not contact the certificate issuer, it can be verified from the system with the help of smart contracts which compare the hash of submitted certificates with the hashes present in the blockchain. With the use of IPFS, a lifelong education portfolio can be created which is secure [10]. Educational certificates on a blockchain must fulfil certain security themes as mentioned in [1]:

1) **Authentication:** The users must be authenticated. The user here can be students, institutes, universities, etc.
2) **Authorization:** Users are provided permission to perform transactions in the blockchain. Eg: The student will be authorized to have full control of the certificate after it is issued by the issuer of the certificate.
3) **Confidentiality:** The private information of the student must be maintained by the academic institute.
4) **Ownership:** The ownership of a digital certificate depends on the users in the blockchain ledger.
5) **Privacy:** Public keys are maintained anonymously.

The above-mentioned themes are important to ensure if the certificate is fake or not. Many implementations have been previously proposed. KMI, OU - UK initiated the use of web reputation, badges and certificates using blockchain as a trusted ledger. These were concentrated on creating blockchains for their use in higher education qualifications in the United Kingdom. Private data was released on a public blockchain which posed a risk. There was also no mechanism that was used to protect the recipient's ownership as well as their privacy. These were a few shortcomings of this implementation [17].

The University of Nicosia made use of bitcoins for many activities [18]. Educational certificates in blockchains were intended to eliminate fraud. They provided software tools using which the users could confirm the authenticity of the certificate. The SHA-256 hashing algorithm is used as a tool for sharing certificates in PDF format. Its shortcomings include that there is no clear method of the authenticity of parties [11]. The use of hash value was also proposed in [12], where the hash value was computed during the document enrollment stage and again during the authentication stage.

MIT Media lab has introduced the use of Blockcerts to issue digital certificates. The issuer firstly signs the digital certificate and then the hash is stored within the blockchain transaction. The recipient of the certificate is then assigned the output of this transaction. This implementation has an issue of ownership and privacy. The level of trust is low. Everyone could access the certificates. The certificates which are stored in the blockchain are tamper proof but it is possible to spoof the certificate. Security and privacy are also a concern in this implementation.

SmartCert [19] is another blockchain based digital credentials verification platform. It is developed to overcome the problem of fake certificates. This system is vulnerable to attacks. With RecordKeeper, certificates can be issued by educational institutes and a receipt can be provided to the user which can then be shared with a third party as a proof of the authenticity of the certificate. There are not many complications in this method, but ownership rights are required by the parties interested in viewing the RecordKeeper blockchain's certificate. This leads to tampering risk, which can arise from the transfer of ownership to a third party. The use of a private blockchain would be better for this method as it would ensure the security of the certificate.

There are many different ways to store the certificates. A database can be maintained to record the certificates where its revocation is also possible and the status of revocation is also stored on the blockchain, which achieves transparency due to its inherent append only feature [13].

In this work, we propose the use of blockchain to verify both students as well as the certificate provided by the student without involving the third party [14]. It is implemented on Ethereum, which is an open-source platform and a public blockchain [15]. Also, there is the need to match student

Authorized licensed use limited to: UT campus at Belfort Montebellard. Downloaded on August 10,2022 at 11:57:30 UTC from IEEE Xplore. Restrictions apply.

identification and the certificate provided, which is also implemented in this work.

III. Proposed Framework

This research has been done keeping in mind the following points:

1) Educational certificates should only be issued by authorized issuing organizations. From a student's point of view, it is very important that the certificates are issued by the university only.
2) Student's data should be secure and confidential. It should be accessible only by the student and the potential verifiers.
3) The functionality of verifying the authenticity of the document should be publicly accessible so that the verifying party does not need access credentials.
4) The verification system should be publicly shared and decentralized. It can be assumed that the system will be persistent and will be available on one of the many decentralized nodes.
5) Technical details involved in the process of issuing certificates should be transparent to all the stakeholders.
6) Smart contracts can be used to automate the response of the verification.

The proposed work has two phases, the First being the Enrollment and Certificate Issuing Phase and the Second is the User and Certificate Verification Phase.

A. Enrollment Process

In the first phase i.e. the enrollment and certificate issuing phase, the following steps are followed:

- Initially, the issuers and recipients are not registered. The issuers are professors or employees of the current college the student is studying in (they will issue the certificate for the students who request them). The recipients are the students of this current college who want to pursue higher studies from another college or want a company job.
- The issuer is asked for fields like Name, email address, phone number, and website while registering.
- The recipient is asked for Name, email, phone number as primary information, and Unique identity number and a unique secret phrase as an identification and security measure during the registration process.
- On the creation of a new issuer or recipient, their information is stored on IPFS and a unique hash is generated which is used as their unique identification. The recipients must store their unique hash as this hash will be used during the verification phase.
- The issuer can generate new certificate types, the details of which are also stored on the IPFS. This certificate also gets a unique hash.
- The recipient can then choose one of the certificates from the list of certificates the issuer has created and request the issuer to issue that certificate for them. After the certificate has been successfully issued for the recipient, they must store the hash of this certificate as well for later use during the verification phase.

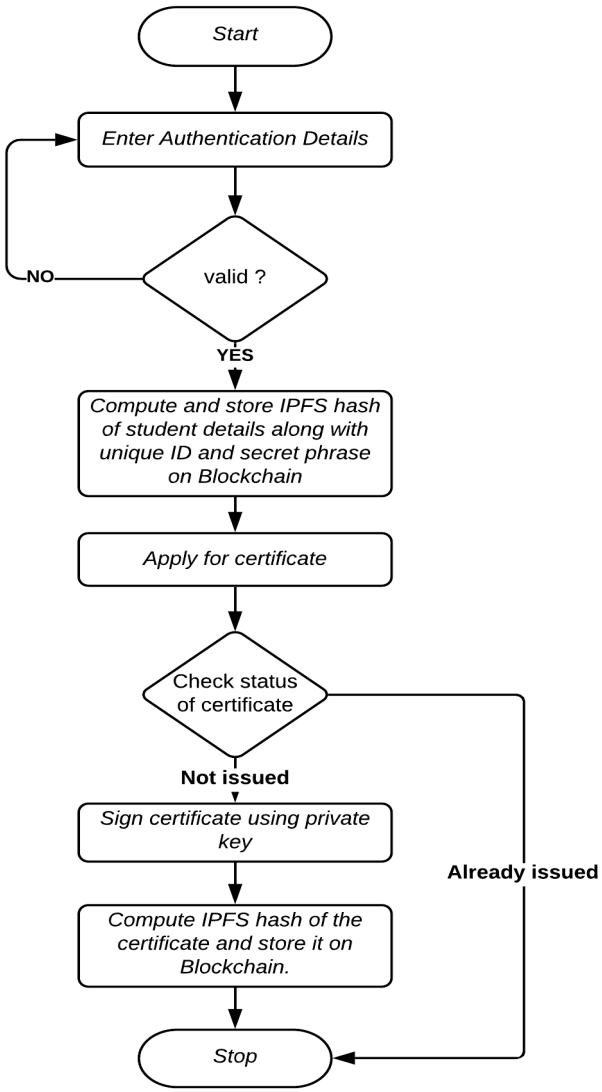

Fig. 1. Certificate Issue Process

Figure 1 explains the Certificate Issuing Process. The student initially enters their credentials and if the student is a valid student, then the hash of the student details and their unique ID and secret phrase are computed and stored on the Blockchain. The student can now request for a certificate to be issued. It is checked if the certificate that the student wants to get issued has been previously issued for him. If the student doesn't already have the certificate, then the college the

Authorized licensed use limited to: UT campus at Belfort Montebellard. Downloaded on August 10,2022 at 11:57:30 UTC from IEEE Xplore. Restrictions apply.

student is currently studying in issues this certificate for the student and signs it using their private key. The hash of the certificate is computed and stored on the Blockchain. With these steps, the student successfully gets the required certificate issued for themselves.

B. Verification Process

Once the required certificates have been issued by the issuer for the user, the second phase is the User and Certificate Verification Phase which has the following steps:

- The student applies to another college for higher education or a company for a job and is required to give their certificates as proof of their skill.
- Members of the new college or employer of the company act as a verifier of the certificates that the student has provided to them. They do not require any third party to perform the verification process for them. They also do not need to register as the issuer and recipients have to.
- The verification process includes three steps:
  - **Student verification:** In this step, user verification happens, i.e., checking if the user is a valid student of the college. Here the user hash is provided, and it is checked from a pool of recipient hashes, and if it exists then the student is valid.
  - **Certificate Verification:** Here the certificate hash is provided by the student to the verifier and it is checked if this certificate hash already exists.
  - **Student-Certificate linkage verification:** The student hash, as well as the certificate hash, are both provided. This will be valid only if the student has been issued this certificate. Just checking if the student is valid and the certificate is valid isn't enough so we check if this valid certificate is actually issued for this valid student or not.
- Once all the above steps are performed the user as well as the user's qualifications are verified.
- All the above steps make use of only the unique hash which is provided by the student for security reasons.

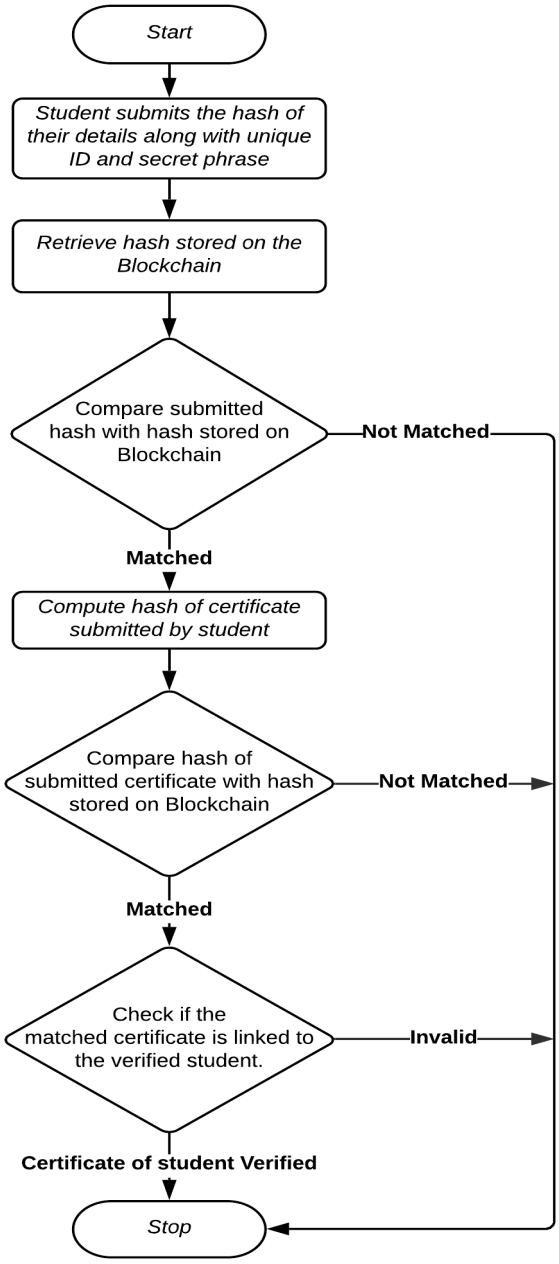

Fig. 2. Verification Process

Once the certificate has been issued for the student, as shown in Figure 1, they use these to apply for jobs or colleges for higher education. The student submits the hash of their details along with the unique identity number and secret phrase to the verifier. If this hash is found on the blockchain, then the student is valid. The student then submits the hash of their certificate and if this hash is present on the blockchain, then the certificate is valid as well. The next step is to check if the verified certificate actually belongs to the verified user. If this linkage is found then these steps complete both the user and certificate verification process. These steps can be seen in Figure 2.

IV. Implementation and Results

This proposed framework has been implemented using various technologies such as Ganache-cli, which was used for setting up a local blockchain and for testing the decentralized application, Truffle for designing and developing the decentralized application, Metamask which connects the web application with the Ethereum blockchain and acts as a bridge between them, and finally IPFS (Interplanetary File System) which is a file sharing system that relies on cryptographic hashes and can be easily stored on the blockchain. Also, a platform was developed as an interface where the proposed framework was tested.

In the implementation, first we connect the certificate management platform to Metamask. After this connection is done, imported accounts can be seen on the platform as shown

Authorized licensed use limited to: UT campus at Belfort Montebellard. Downloaded on August 10,2022 at 11:57:30 UTC from IEEE Xplore. Restrictions apply.

Fig. 3. Screenshots of the implemented system: (a) Account connected with web application, (b) Issuer registration page, (c) Issuer Page, (d) Recipient registration page, (e) Recipient Page, and (f) Verification Process

in Figure 3a. These accounts can now be used to perform transactions.

Once the Metamask has been connected with the certificate management platform, the issuer as well as recipients have to register themselves. The issuer has to fill various fields such as Name, Email ID, Phone Number and URL to get registered as shown in Figure 3b. After the issuer has registered another page appears (Figure 3c) where they can use the Register certificate to register for new certificates and then issue these certificates for the recipient who has requests for them.

The recipient also has to fill fields such as Name, Email ID, Phone Number as their main information along with Unique ID (Eg: Aadhar Number) and secret phrase as security information to register, as can be seen in Figure 3d. Once the recipient has registered, they can view all the certificates that have been issued to them and by whom they were issued (Figure 3e).

The above two pages, i.e. issuer and recipient registration pages require the users to login but in case of the verifier, they must have a page that has no login as they are a third party. Thus, a third page is created for the verifier which can act as an Information desk that they can use to perform the three-step verification process, which had been discussed in the methodology above. A sample result for correct hash values entered can be seen in Figure 3f. If all three checks give valid as their result, then the user, as well as users certificates, are valid.

V. Conclusion

In this work, we have implemented a blockchain based educational certificate verification system. It also adds another security layer by verifying the student. Both the student identity and certificate are verified by calculating their hashes and finding a match in the hashes present in the blockchain. The current work makes use of a student's unique identity number or biometric along with a unique secret phrase for

Authorized licensed use limited to: UT campus at Belfort Montebellard. Downloaded on August 10,2022 at 11:57:30 UTC from IEEE Xplore. Restrictions apply.

User verification and using the hash of the certificate provided by the student for Certificate Verification.

The novelty of the proposed work is to link the certificates to the user identity for more security and to make a fool-proof system. The certificates are verified only if the certificate is found to match the student's actual identity and not just the name of the student. Future work can be to easily implement a functionality for employers to calculate the hash of the students' documents.

References

[1] Saleh, O.S., Ghazali, O. and Rana, M.E., 2020. Blockchain based framework for educational certificates verification. In Studies, Planning and Follow-up Directorate. Ministry of Higher Education and Scientific Research, Baghdad, Iraq. School of Computing, University Utara Malaysia.

[2] Namasudra, S., Deka, G.C., Johri, P., Hosseinpour, M. and Gandomi, A.H., 2020. The revolution of blockchain: State-of-the-art and research challenges. Archives of Computational Methods in Engineering, pp.1-19.

[3] Saleh, O.S., Graduation Certificate Verification Model: A Preliminary Study.

[4] Balsubramanian, S., Prashanth, I.R. and Ravishankar, S., 2009, August. Mark sheet verification. In 2009 3rd International Conference on Anticounterfeiting, Security, and Identification in Communication (pp. 359- 362). IEEE.

[5] Salleh, M. and Yew, T.C., 2009, June. Application of 2D barcode in hardcopy document verification system. In International Conference on Information Security and Assurance (pp. 644-651). Springer, Berlin, Heidelberg.

[6] Baldi, M., Chiaraluce, F., Frontoni, E., Gottardi, G., Sciarroni, D. and Spalazzi, L., 2017, January. Certificate Validation Through Public Ledgers and Blockchains. In ITASEC (pp. 156-165).

[7] Mudliar, K., Parekh, H. and Bhavathankar, P., 2018, February. A comprehensive integration of national identity with blockchain technology. In 2018 International Conference on Communication information and Computing Technology (ICCICT) (pp. 1-6). IEEE.

[8] Gao, Z., Xu, L., Turner, G., Patel, B., Diallo, N., Chen, L. and Shi, W., 2018, June. Blockchain-based identity management with mobile device. In Proceedings of the 1st Workshop on Cryptocurrencies and Blockchains for Distributed Systems (pp. 66-70).

[9] Liu, Y., Sun, G. and Schuckers, S., 2019, June. Enabling Secure and Privacy Preserving Identity Management via Smart Contract. In 2019 IEEE Conference on Communications and Network Security (CNS) (pp. 1-8). IEEE.

[10] Guo, J., Li, C., Zhang, G., Sun, Y. and Bie, R., 2019. Blockchain-enabled digital rights management for multimedia resources of online education. Multimedia Tools and Applications, pp.1-21.

[11] Bond, F., Amati, F. and Blousson, G., 2015. Blockchain, academic verification use case. Buenos Aires.

[12] Voloshynovskiy, S., Koval, O., Villan, R., Topak, E., Forcen, J.E.V., ´ Deguillaume, F., Rytsar, Y. and Pun, T., 2006, February. Informationtheoretic analysis of electronic and printed document authentication. In Security, Steganography, and Watermarking of Multimedia Contents VIII (Vol. 6072, p. 60721D). International Society for Optics and Photonics.

[13] Wang, Z., Lin, J., Cai, Q., Wang, Q., Zha, D. and Jing, J., 2020. Blockchain-based certificate transparency and revocation transparency. IEEE Transactions on Dependable and Secure Computing.

[14] Dalal, J., Chaturvedi, M., Gandre, H. and Thombare, S., 2020. Verification of Identity and Educational Certificates of Students Using Biometric and Blockchain. Available at SSRN 3564638.

[15] Cheng, J.C., Lee, N.Y., Chi, C. and 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.

[16] Baldi, M., Chiaraluce, F., Frontoni, E., Gottardi, G., Sciarroni, D. and Spalazzi, L., 2017, January. Certificate Validation Through Public Ledgers and Blockchains. In ITASEC (pp. 156-165).

[17] J. Domingue, 2017. Blockchains as a Component of the Next Generation Internet.

[18] Yessi Bello Perez. The Global Universities embracing cryptocurrency.

[19] R.G. and M.K.S. Sharma, P. Pathak, 2017. Blockchain imperative for educational certificates.

[20] Sivaganesan, D., 2020. Smart Contract Based Industrial Data Preservation on Block Chain. Journal of Ubiquitous Computing and Communication Technologies (UCCT), 2(01), pp.39-47.

Authorized licensed use limited to: UT campus at Belfort Montebellard. Downloaded on August 10,2022 at 11:57:30 UTC from IEEE Xplore. Restrictions apply.