e-ISSN: 2582-5208

International Research Journal of Modernization in Engineering Technology and Science

(Peer-Reviewed, Open Access, Fully Refereed International Journal)

Volume:04/Issue:07/July-2022 Impact Factor- 6.752 www.irjmets.com

BLOCKCHAIN BASED CERTIFICATE VALIDATION SYSTEM

Mrs. R. Suganthalakshmi*1, Mrs. G. Chandra Praba*2, Mrs. K. Abhirami*3, Mrs. S. Puvaneswari*4

*1,2,3,4Asst Prof, Department CSE, Kings College Of Engineering,
Pudukottai, Tamil Nadu, India.

ABSTRACT

Education is necessary for each and everyone. During the course of education, the students achieve many certificates. With their certificates they can apply for job at public or private sectors, where all these certificates are needed to be verified manually. There can be incidents where students may produce fake certificate and it is difficult to identify them. This problem of fake academic certificates has been a longstanding issue in the academic community. To make the data more secure and safe, everything needs to be digitalized with the principle of Confidentiality, Reliability, and Availability. All of these can be achieved with a technology named Block chain. The Block chain technology provides inherent security quality where it can be used to generate the digital certificate which is anti-counterfeit and easy to verify. Each certificate will have a unique hash key which can be used to validate the authenticity of the certificate by any organization through the portal. The benefit this a system is that the student also faces less risk of losing or damaging a certificate and the validation of the certificate can also be done quite easily.

Keywords: Block Chain, Digital Certificates, Confidentiality, Reliability, Availability.

I. INTRODUCTION

In India, usually a student's studies goes like taking admission in kindergarten, after that changing of school for primary, secondary, and high school studies. After completing high school students, need to get admission into college. For graduation, there's also once again changing of college. This is the basic cycle for student's study years. After this, some students continue to pursue higher studies. So the problem with this cycle is that a student needs to produce all his certificates in each stage for validation. This poses a risk of losing and damaging the certificate. And it is tedious for the validator to authenticate each certificate. With such a huge population in our country, almost every year 26.3 million students graduate. It is very hard to keep track and validate such a huge amount of records. Due to this, an unwanted scenario rises i.e. tampering and production of fake or duplicate certificates. There are a lot of hidden agencies in our country who are running this scam behind everyone's back. Technology has moved quite forward until now. Distinguishing between a fake and an original certificate will require a lot of concentration and result in wastage of precious time.

For removing this disadvantage, a technology named Blockchain comes into our life as a savior. The data in a Blockchain cannot be changed under realistic conditions. Even if data is changed, it just takes a second to let us know about the tampering. In Blockchain a data or a node is validated only when multiple parties approve it. So, the system would be Reliable and Authenticated at any instance of time. Now, the issue of tampering is solved.

Certificates distributed in colleges or universities are mostly in the form of hard copy. Whenever applicants apply for the job at any public or private sector they have to produce those hard copies, while the organizations have to verify all certificates manually which is very time-consuming process and there are chances that some may have produce the certificate which is not legit and that may get unnoticed by the verifier during the process because of this ineligible candidate will get a chance. There had been lot of cases in past where people are caught selling fake certificates of different organization at low cost. To eradicate such problem and diminish the production of fake certificates we can use the Blockchain technology. Blockchain can be used to store the data of the certificate that can be validated by anyone from any place.

The Blockchain is a decentralized shared distributed ledger; the data stored in the Blockchain is almost un-modifiable. It is a type of database which is not centralized and governed by the set of rules. In this study, we are going to develop the decentralized certificate verification application on the Blockchain. We are selecting this technology because it is traceable, tamper proof and encrypted. By integrating the Blockchain technology we will be able to eradicate the problem of fake certificates. We will use smart contract at backend to interact with the Blockchain and the encrypted hash value of each document will be stored in Blockchain which will be verified against the user document. This proposed system not only removes the loopholes in our current system but also gives us an effective and concrete solution.

II. PROPOSED SYSTEM

A. Methodology

In this proposed system, the academic certificates are converted into digital form. The institute register itself and register the students. They upload each student's certificate. The consensus algorithm is used for generating the hash values. In the Blockchain, each block consists of hash value, timestamp, previous hash value and they connected together. The user verifies the certificates by using the login id and password of the student created by the institution.

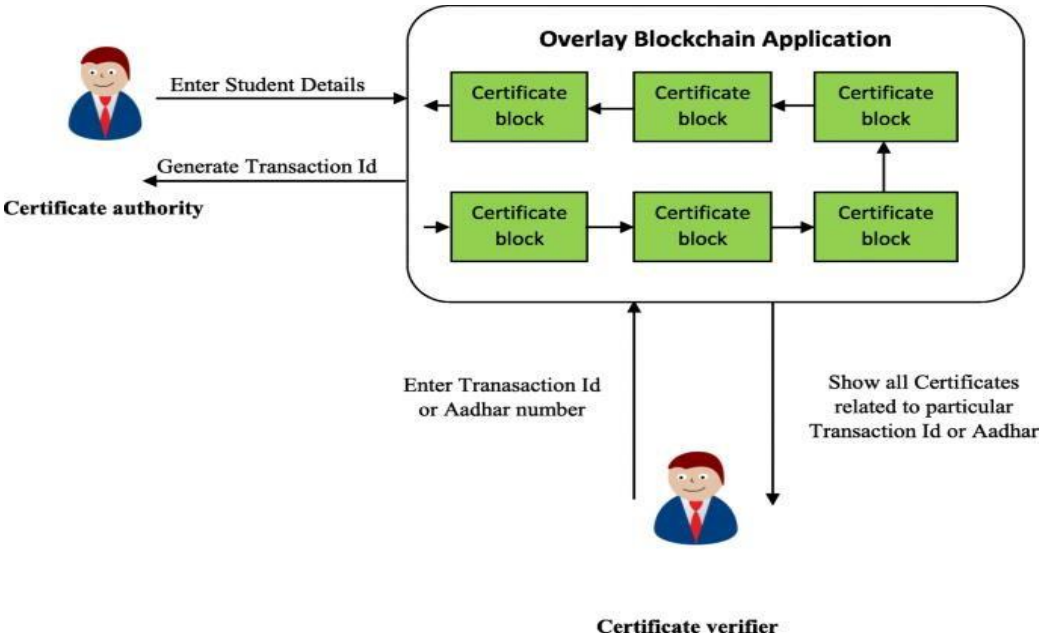


Figure 1: Architecture Diagram

B. Digital Certificate Creation

The student's certificates are converted into digital form by using our mobile camera. By using the admin login, the Institution login to our application. Then they register the students by using their name, email, mobile number and they create a user id and password for them. They upload the certificates scanned by the mobile camera. In the next page, they can add student and their certificates.

C. Hash value Generation

The SHA-256 algorithm is used for generating the hash value for the certificates. It accepts input in various sizes and produces a fixed size hash value. When the certificate gets uploaded, the hash value is generated.

D. Certificate validation

The certificates are stored in Blockchain. They are validated by using the Proof Of Work Consensus algorithm. This consensus algorithm is used to select a miner block. The user should login to our application by their login Id and Password. They may view the certificates of the students by entering the student's Id and Password. If that particular student is available, it will show the name of the student and his certificates. If the student is not available it will shows the error message.

E. Working of Application

To create the block chain based unmodifiable certificates, initially the college needs to get registered. Each college will be having its wallet address from which it is going to send transaction. Colleges can be added only by the owner of the smart contract. Once the college gets registered, they should login to the application and register students. The students were registered by their unique ID(Aadhar). The institute will create a password for them. After the registration of students, the certificates are uploaded by the Institution.

III. RESULTS & DISCUSSIONS

A. INSTITUTION LOGIN

i) Registration

- To create the block chain based unmodifiable certificates, initially the college needs to get registered.
- Each college will be having its wallet address from which it is going to send transaction.
- Colleges can be added only by the owner of the smart contract.

ii) Student Registration

- Once the college gets registered, they should login to the application and register students.
- The students were registered by their unique ID(Aadhar).
- The institute will create a password for them.
- The details of the students and their certificates are stored in the database.

B. UPLOAD CERTIFICATES

- After registration of students, the digital certificates are uploaded by the Institution.
- Then hash value for each certificate is generated by using **SHA-256** algorithm.
- SHA-256 (secure hash algorithm, FIPS 182-2) is a cryptographic hash function with digest length of 256 bits.
- It is a keyless hash function; that is, an MDC (Manipulation Detection Code).
- Each certificate is processed by blocks of 512 = 16 × 32 bits, each block requiring 64 rounds.
- It finally provides a common length of hash value.

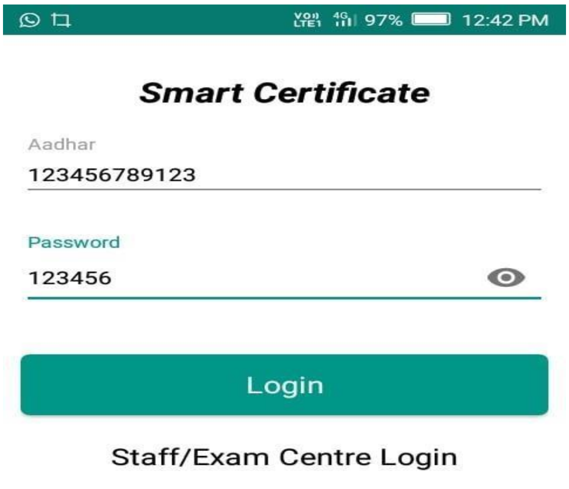
C. USER LOGIN

i) View

- The company or students may view the certificates by entering their unique ID and password created by the Institute.

ii) Validation

- If we scan a certificate, the application should validate it and provide a result about the certificate availability.
- Each certificate added to the blockchain by the working of consensus algorithm.
- A consensus algorithm is a procedure through which all the peers of the blockchain network reach a common agreement about the present state of the distributed ledger.
- Proof of Work (PoW) consensus algorithm is used for adding hash value of the certificates to the block.
- It performs some computation work by using the hash value, timestamp and the user id.



Aadhar
123456789123

Password
123456

Staff/Exam Centre Login

Figure 2: Staff/Exam Center Login

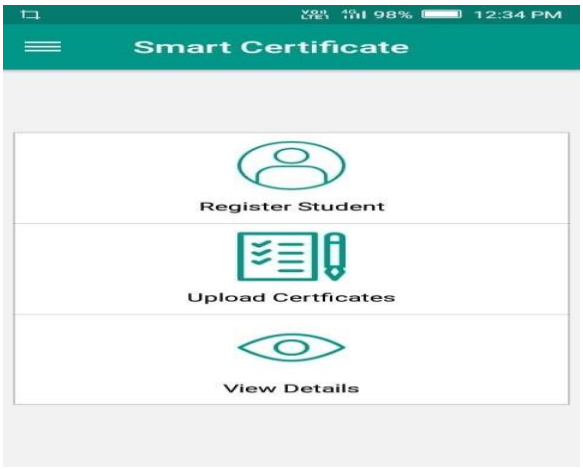
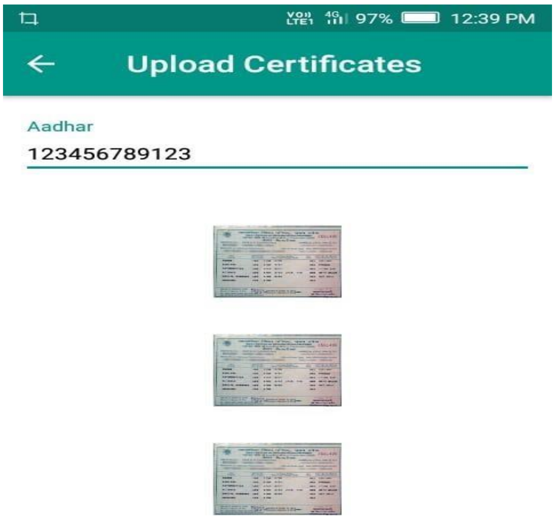
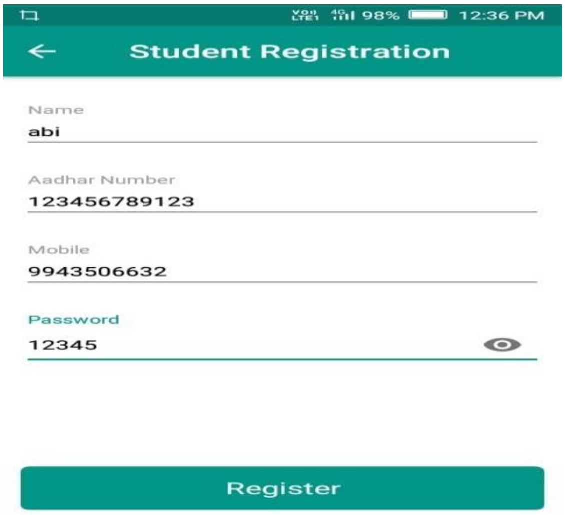


Figure 3: Students View



Upload Certificates

Aadhar
123456789123



Student Registration

Name
abi

Aadhar Number
123456789123

Mobile
9943506632

Password
12345

Figure 4: Students Registration

Figure 5: Certificate Uploading

IV. CONCLUSION

In this paper, we proposed a solution for document forgery. By integrating Blockchain technology, we will able to eradicate the problem of fake certificates and certificates missing. We can view our certificates from anywhere at any time. The application provides accurate and reliable information of digital certificates.

V. REFERENCES

[1] C. K. Wong and S, S. Lam "Digital signatures for flows and multicasts", WEEE/ACM Transactions on Networking, 7(4): 502- 513, 1999.

[2] A. M. Antonopoulos, Mastering Bitcoin: Unlocking Digital. Sebastopol, CA, USA: O'Reilly Media, 2015.

[3] Benyuan He, "An Empirical Study of Online Shopping Using Blockchain Technology", Department of Distribution Management, Takming University of Science and Technology, Taiwan, R.O.C., 2017.

[4] Chris Dannen, Introducing Ethereum and Solidity,
https://www.apress.com/br/book/9781484225349

[5] J. Clark and P. C. van Oorschot, "SoK: SSL and HTTPS: Revisiting past challenges and evaluating certificate trust model enhancements," in proc. IEEE S&P'13, May 2013, pp. 511–525.

[6] L. Zhang, D. Choffnes, D. Levin,et al., "Analysis of SSL certificate reissues and revocations in the wake of Heartbleed," in proc. ACMIMC'14, Nov 2014, pp. 489– 502.

[7] M. Carvalho and R. Ford, "Moving-target defenses for computer networks," IEEE Security & Privacy, vol. 12, no. 2, pp. 73–76, Mar.-Apr.2014.

[8] Papazoglou, M., Service-Orientated Computing: Concepts, Characteristics and Directions, in International Conference on Web Information Systems Engineering. 2003, IEEE: Rome.

[9] D. Ferraiolo, R. Kuhn, and R. Sandhu, "Rbac standard rationale: Comments on "a critique of the ansi standard on role-based access control", "IEEE Security Privacy, vol. 5, no. 6, pp. 51–53, Nov 2007.

[10] A. Ouaddah, A. A. Elkalam, and A. A. Ouahman, "Towards a novel privacy- preserving access control model based on blockchain technology in IOT," in Europe and MENA Cooperation Advances in Information and Communication Technologies. Springer, 2017, pp. 523– 533.

[11] L. Y. Chen and H. P. Reiser, "Distributed applications and interoperable systems, 17th ifip wg 6.1 international conference, dais 2017, held as part of the 12th international federated conference on distributed computing techniques, discotec 2017, neuchtel, switzerland, June 1922, 2017." Springer, 2017.

[12] Q. Xia, E. B. Sifah, K. O. Asamoah, J. Gao, X. Du, and M. Guizani, "Medshare: Trust-less medical data sharing among cloud service providers via blockchain," IEEE Access, vol. 5, pp. 14 757–14 767, 2017.