Blockchain based Certificate Validation System

Vrushank Rao*[1], Vinay Kumar M*[2], KC Sri Venkatesh*[3]
*[123]Student, Department of Computer science and Engineering, Presidency
University, Yelhanka, Bangalore, India

Abstract:- Education is necessary for every individual. During the course of training, students obtain numerous certificates. You can use your certificates to apply for jobs in the public or private sector, but all of these certificates must be manually verified. Students may present fake certificates, which can be difficult to identify. The issue of academic falsification has been a long-standing issue in the academic world.

To make your data more secure, everything should be digitized according to the principles of confidentiality, reliability, and availability. All of this can be achieved using a technology called blockchain. Blockchain technology offers inherent security qualities and can be used to generate digital certificates that are tamper-proof and easy to verify. Each certificate has a unique hash key that any organization can use through the portal to verify the certificate's authenticity. The advantage of this system is that there is less risk of students losing or damaging their certificates, and certificate verification is also very easy.

***Keywords:-** Blockchain, Digital Certificates, Confidentiality, Reliability, Availability.*

I. INTRODUCTION

In India, a student's learning is typically like starting kindergarten and then transferring to elementary school, middle school, and high school. After graduating from high school, students must enroll in college. Finally, there is the possibility of changing universities. This is the basic cycle of a student's academic year. Some students then go on to further education. So the problem with this cycle is that at each stage students have to submit all their certificates for verification. Certificates may be lost or damaged. Also, it is cumbersome for the verifier to authenticate each certificate. Our country has such a large population that approximately 26.3 million students graduate each year. Tracking and validating such large datasets is extremely difficult.

This leads to the undesirable scenario of manipulating or creating fake or duplicate certificates. There are many hidden agencies in our country that carry out this fraud hidden from everyone.

Technology has come a long way so far.Distinguishing between fake and genuine certificates requires a lot of concentration and wastes valuable time.

To eliminate this disadvantage, a technology called blockchain appears in our lives as a savior.

Under realistic conditions, the data in the blockchain cannot be changed.

Even if the data is changed, it only takes one second to know that it has been tampered with.

In blockchain, data or nodes are only verified if multiple parties approve them.Therefore, the system is reliable and always authenticated.This will resolve the operation issue.

Certificates distributed by universities are usually in paper format.

When an applicant applies for a job in the public or private sector, the applicant has to submit it in paper form, but the organization has to manually check all the certificates, which is very It is a time-consuming process and some companies may submit certificates such as: The examiner may not notice this during the process because the case is legitimate and this unqualified candidate is given a chance.

In the past, there have been many cases where people have been arrested for selling fake certificates of various organizations at low cost.

Blockchain technology can be used to solve this problem and reduce the creation of fake certificates.

Blockchain can be used to store and verify certificate data 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 Eliminate the problem of fake certificates.A smart contract is used on the backend to interact with the blockchain, and the encrypted hash value of each document is stored on the blockchain and verified against the user's document. This proposed system not only addresses the gaps in the current system but also provides effective and concrete solutions.

II. PROPOSED SYSTEM

A. Methodology

Building a blockchain based certificate validation project means leveraging a decentralized and tamper proof nature of blockchain technology to ensure authenticity and integrity of certificates.Below describe the main components of the project: [13]

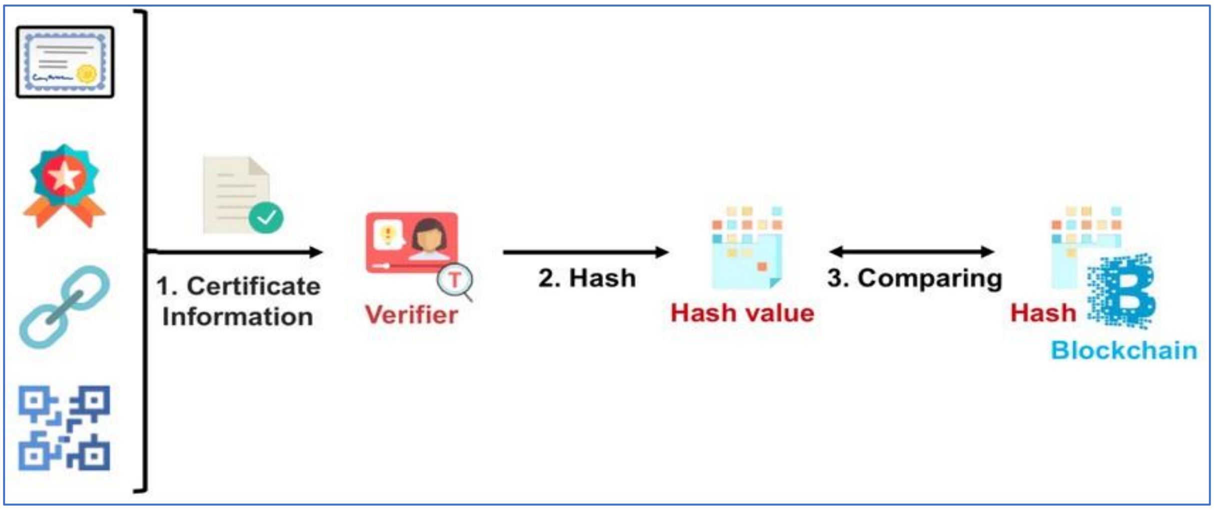

Fig. 1: Verification process.

B. Name:

Refers the name of the certificate owner.We are inserting a field in the certificate data structure to store name of person who purchase a certificate.This part of information becomes the transaction recorded on the blockchain.

C. Course:

Specifies the course or program for which the certificate is awarded.It creates field in the certificate data structure to store course details.This field contains information such as course name,duration and other relevant details.

D. Issuing Organization:

Identifies the organization or authority that issues the certificate.Includes a field in certificate data structure that captures about issuing organization.

E. Certificate Hash:

We use cryptographic hashes of certificate data to ensure data integrity.Create a unique identifier by generating a hash (e.g.SHA-256) of the entire certificate data, including name, course, issuing organization, and other relevant details. Storing this hash on the blockchain ensures that the record is tamper-proof.It is important to note that any changes to the certificate data will generate a different hash, highlighting potential tampering attempts.

F. Certificate

- *ID:*

Each certificate requires a unique identifier to facilitate search and verification.

To address this issue, we assign a unique certificate ID to each certificate at the time of issuance. This unique ID becomes an integral part of the blockchain record, ensuring easy search and quick verification.

G. Working of Application:

- *Certificate Issued:*

When a certificate is issued, details such as the owner's name, course, and issuing organization are captured. These details are hashed to create a unique certificate identifier.The hashed data is securely stored on the blockchain along with the assigned certificate ID.

H. Blockchain Storage:

Blockchain acts as a distributed ledger and stores all certificates and their corresponding hashed details.Each block in the blockchain contains a set of certificates, creating a comprehensive and transparent repository.The blockchain network's nodes collectively store the certificate details in a decentralized fashion, including the Certificate ID, Certificate Hash, and other pertinent data.The fields for the name of the individual, the completed course, the details of the issuing organization, and any additional metadata are defined in the certificate data structure. Consistency and effective validation are guaranteed by this organized data.A certificate's details cannot be changed or removed once they are recorded due to the decentralized and immutable nature of the blockchain. The validation process's integrity is strengthened by its permanence.

I. Certificate Validation:

To validate a certificate, a user provides a certificate ID.The application uses this ID to retrieve the corresponding hashed data from the blockchain.At the same time, the certificate details provided by the user are hashed and the resulting hash is compared with the hash stored on the blockchain.If the hashes match, the certificate is considered authentic and valid.If there is a mismatch, this indicates possible tampering or manipulation of the certificate data and advises the user to be careful.

III. RESULTS AND DISCUSSIONS

Blockchain-based certificate verification projects leverage the decentralized and tamperproof nature of blockchain technology.When an individual completes a course, the issuing organization creates a unique certificate that includes the individual's name, the completed course, and the issuing organization's details. This certificate is assigned a certificate ID, and its contents are hashed using a cryptographic algorithm to create a digital fingerprint called a certificate hash.This data is stored on the blockchain via smart contracts, ensuring transparency and immutability.To verify a certificate, users provide either the certificate ID or the certificate hash.The smart contract retrieves the relevant certificate details from the blockchain and recalculates the hash from the provided information.If the recalculated hash matches the stored hash, the certificate is considered authentic, providing a secure, efficient, and decentralized method of certificate verification.

Table 1: Result obtained vs Existing Methods

Criteria	Blockchain-Based Certificate Validation	Existing Methods
Security	Uses decentralization and cryptographic hashing to provide tamper resistance. Data integrity is ensured by immutability.	Conventional techniques might entail actual certificates bearing seals and signatures. Secure databases and encryption are used in digital methods.
Transparency	Provides a decentralized ledger with high transparency, boosting stakeholder trust.	Transparency may be lacking in traditional certificates. Transparency is achieved through centralized databases in digital methods.
Efficiency	Effective verification with a hash or Certificate ID. Reliance on central authorities is decreased through decentralization.	Manual verification procedures might be necessary for traditional methods. Validation via online platforms can be streamlined with digital methods.
Adoption Potential	Offers a forward-thinking solution, particularly in sectors where credential validation and trust are valued.	Digital methods are frequently utilized; traditional methods are deeply ingrained. Adoption might be contingent upon industry readiness to accept blockchain.
Consideration and Challenges	The consensus process and blockchain platform are key components of security. Scalability could be a problem.	Physical certificates are prone to being misplaced or destroyed. Issues with standardization and interoperability may arise with digital methods.

IV. CONCLUSION

In this paper, we proposed a solution to document forgery. Integrating blockchain technology can eliminate the issue of forged or lost certificates. Check your certificates anytime, anywhere. This application provides accurate and reliable information about digital certificates. A blockchain-based certificate validation project includes key elements such as name, course, issuing organization, certificate hash, certificate ID, etc., and issues security, reliability, and efficiency in the certificate validation process. Provides a robust solution to address By using decentralized blockchain technology, this project ensures the integrity and immutability of certificates, thereby significantly reducing the risk of fraud. Certificate ID allows you to quickly and reliably retrieve certificate details, simplifying the verification process for various parties. A cryptographic hash of the certificate content provides a tamper-proof mechanism that enhances the overall security of the system. This innovative approach not only minimizes dependence on central authorities, but also promotes transparency and trust in validating education and training qualifications. As projects evolve, collaboration with stakeholders, compliance with regulatory standards, and a focus on user-friendly interfaces will be essential to widespread adoption and success in the certificate validation space.

REFERENCES

[1]. The Proposal of a Blockchain-based Architecture for Transparent Certificate Handling, J. Gresch, B. Rodrigues, E. Scheid, S. S. Kanhere, and B. Stiller, BIS2018: Business Information System. Workshops, vol. 339 of Lecture Notes in Business Information Processing, Springer, pp. 185-196, 2018.

[2]. Jayachitra, J., Matilda, S., and Gayathiri, A. (2020). Blockchain-based certificate validation. The seventh international conference on smart structures and systems (ICSSS) is scheduled for 2020.http://10.1109/icsss49621.2020.9201988

[3]. Carlos Enrique Montenegro-Marin and Song, Hesheng. "Secure prediction and assessment of sports injuries using deep learning based convolutional neural network." 12.3 (2021): 3399-3410 in Journal of Ambient Intelligence and Humanized Computing.

[4]. Jinping Chang, Sujatha Krishnamoorthy, and Seifedine Nimer Kadry. "Review and synthesis of Big Data analytics and computing for smart sustainable cities." Smart Transportation Systems, IET (2020).

[5]. "Behavior-based swarm model using fuzzy controller for route planning and E-waste collection," Batoo, Khalid Mujasam, et al. Pollution Research and Environmental Science, 2021, 1–15.

[6]. L.Zhang, D.Choffnes, D.Levin et al., "Analysis of SSL certificate reissue and revocation during Heartbleed," Procedures ACMIMC'14, November 2014, p.489–502.

[7]. M.Carvalho and R.Ford, "Moving target defense for computer networks," IEEE Security & Privacy, vol.12, Nine.2, S.73–76, Ma rz-April 2014.

[8]. Papazoglou, M., Service-oriented computing: concepts, characteristics, and directions, International Conference on Web Information Systems Engineering.2003, IEEE: Rom.

[9]. D.Ferraiolo, R.Kuhn, and R.Sandhu, "Rbac Standard Rationale: Comments on "A Critique of the ANSI Standard for role-based Access Control," IEEE Security Privacy, vol. 5, no.6, p.51–53, November 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," Information and Communication Technology Advances in Europe and MENA Cooperation.Springer, 2017, S.523–533.

[11]. L.Y.Chen and H.P.Reiser, "Distributed Applications and Interoperable Systems, 17th International

Conference Held as Part of the 12th International Conference on Distributed Computing Technologies ifip wg 6.1, Lectern 2017, Discotec 2017, Neuchter, Switzerland., June 1922, 2017"Springer, 2017.

[12]. Q.Shea, E.B.Shifa, K.O.Asamoah, J.Gao, X. Du, and M.Guizani, "Medshare: Trustless exchange of medical data between cloud service providers over blockchain," IEEE Access, vol. 5, 14 757–14 767, 2017.

[13]. Nguyen Huynh-Tuong, Hoang-Anh Pham "CVSS: Blockchained Certificate Verification Support System" https: //www.researchgate.net/publication/329139747