

Decentralized Certificate Verification Application via blockchain-A Review

Priya Shelke¹, Mayank Sahu², Ekta Mulkalwar³, Siddhesh Kothadi⁴ and Shantanu Kawade⁵

¹⁻⁵Vishwakarma Institute of Information Technology/Information Technology, Pune, India

Email: {priya.shelke, mayank.21910632, ekta.21910986, siddhesh.21910416, shantanu.21911180}@viit.ac.in

Abstract—With an increase in demand for online education and online services in general, there has also been an increase in the move from doing things in the traditional manner to doing things online. The market for online certifications is one of these "online services" key segments. The importance of certificates in the online world has increased significantly, whether they are issued by educational institutions or corporate businesses that may need to validate the competence of their staff. The worry about confirming the authenticity of the certificate itself is growing along with the need for online certification technologies. Since the blockchain network uses distributed ledger technology and each block of data contains a cryptographic hash of the previous block, we plan to use it to apply this certification technology in our project.

Index Terms— blockchain, hash, ledger technology and online certifications.

I. INTRODUCTION

The advancement of information technology, the widespread use of the Internet, and the use of mobile devices have all revolutionized how people live. Virtual cash, often known as digital coins, was primarily developed for use online but is now frequently utilized offline. Many virtual currencies, including the most well-known ones like Bitcoin, Ether, and Ripple, whose value has recently risen, have found popularity thanks to the convenience of the Internet. The blockchain, the primary technology underlying these cutting-edge currencies, is beginning to draw interest. Blockchain has a decentralized, impenetrable database with numerous potential uses.

Certificates can be used for authentication, achievement evidence, and membership. It may be given out by a reputable member of the community. Its civilization has developed as a result of its alleged indestructibility. The claim stated in the certificate can be accepted without the necessity for verification with the issuing body thanks to the unforgeability assumption. This results in considerable time and resource savings. But since certificates are now easily falsified, it is now feasible to enter most institutions, apply for government positions, and do other things using a false identity, which can occasionally have major consequences. The present analog-based certificate management system is sluggish and unstable.

In our project, we intend to upload certificates as JSON objects to the IPFS network, which, like BitTorrent, allows users to host and receive content. In contrast to a centralized server, IPFS is built on a decentralized network of user operators who each own a fraction of the total data, making it a powerful method for sharing and storing files. Any user on the network is able to serve a file by its content address (DHT), and we use an IPFS gateway, such as piata or infra, to establish a connection. Using a distributed hash table, other peers in the network can find and request that content from any node that possesses it. In this case, the IPFS Gateway acts as

a bridge between traditional web browsers and IPFS. Through the gateway, users can access files and websites saved in IPFS as if they were stored in a conventional web server.

II. LITERATURE SURVEY

Building an immutable certificate generation and validation system is the project's main goal. To support this, we cited a few previously published articles and publications by prominent experts on the subject. Blockchain technology, a cutting-edge storage system, and digital certificate validations were the major topics of our literature review.

Tamper Proof Certificate Management System [1] has been proposed to create and validate certificates. The researchers suggested using a blockchain network based on the hyperledger fabric. The IPFS receives the certificates as JSON objects, allowing users to easily share their certificates for verification by saving the certificate information on IPFS.

Revocation mechanisms for academic certificates stored on a blockchain [2] propose a novel technique for revoking certificates generated by a blockchain system. In addition to a certificate's IPFS upload, they suggest having a complementary JSON object that is pinned to the IPFS separately. This extra JSON file can be used to revoke the certificate if necessary. However, the article does not provide a suitable technique for confirming the legitimacy of the user making changes to the JSON file.

Ethereum-Block chain-Based Technology of Decentralized Smart Contract Certificate System [3] has been proposed for the innovation and entrepreneurship of college students. The system includes a set of blockchain certificate services in a smart contract, and provides two operating modes: with and without a third-level authority system. If the private key is misplaced or compromised, the three-level authority management system may fail.

A Verified Ethereum-Based Smart Contract Model to Detect Counterfeit Educational Certificate [4] has been proposed, based on the Ethereum (EVM) platform. The system consists of three components: smart contract verification, the E-Cert platform, and student registration. This allows employees to identify fake certifications without the need for a middleman or other third party. However, the implementation of this system may be costly due to its complexity and the higher transaction expenses.

Certificate Verification using Blockchain and Generation of Transcript [5] has been proposed. The solution uses distributed technologies like IPFS and Ethereum smart contracts to make it easy to determine whether a document is authentic and to check its integrity and originality. The use of an additional hashing algorithm reduces the amount of data that can be altered.

Decentralization of Credential Verification System using Blockchain [6] has been proposed. In addition to keeping the digitally signed transactions on the blockchain network, the system also issues certificates to students. The certified documents sent by the students to companies or authorities include a QR code and a special number that can be used by those organizations to validate the certificates. Compared to previous blockchain-based technologies suggested in the literature and by industry, the proposed system offers a number of advantages.

A framework and smart contract for a blockchain-enabled certificate verification system using robotics has been proposed in [7]. This system uses robotic cameras to scan certificates and save them in the cloud using a WiFi-connected Arduino Uno. The same data is then stored on the blockchain in the form of blocks and verified by smart contracts. The main advantage of using robots is that once it is set up, it can scan certificates without human intervention.

A knowledge engineering-based DApp using blockchain technology for protecting the privacy of medical certificates has been proposed in [8]. Traditional methods of storing medical certificates, such as paper, databases, or the cloud, are vulnerable to attacks. This study describes a DApp expert system for maintaining official health records, including medical certificates, using public blockchain technology. The DApp acts as a bridge between systems for issuing medical certificates, intelligent agents, and blockchains. The proposed system is secure, distributed, transparent, and immutable, and is built using blockchain technology. It can thwart attacks and scams using legitimate medical documents. Only authorized stakeholders are permitted to perform operations under this system. However, this system does not currently support picture documents.

A system for creating electronic certificates using information about current students and fog computing has been proposed in [9]. Fog computing, also known as fog networking or fogging, involves moving cutting-edge computing applications, data, and services away from centralized cloud systems and toward the edge of the network. With the help of edge server nodes, the fog computing architecture can be characterized as a highly

virtualized computing infrastructure that provides hierarchical computing resources. These fog nodes coordinate a range of services and applications to process and store content near to end users.

The Digital Certificate System for Verification of Educational Certificates Using Blockchain [10] proposes a dynamic certificate-generating approach using a proprietary blockchain. Students first apply for an e-certificate on a web portal with their educational documents, and a third party verifies the university documents. A unique certificate ID is issued for the student and made available to companies once the data has been properly validated and saved on the blockchain.

The Online Certificate Validation Using Blockchain [11] system is run by the Ethereum Virtual Machine (EVM) and was created on the Ethereum platform. The system is open and transparent about the automatic certificate-giving and application processes, so businesses or organizations can query the system for information about any certificate. The system guarantees the security and accuracy of the information.

The Blockchain-based Platform for Secure Sharing and Validation of Vaccination Certificates [12] discusses the design and implementation of a blockchain-based system for digital immunization and testing certificates. The proposed system uses Ethereum and incorporates self-sovereign identity (SSI) and strong security design principles into its smart contracts. The system enables secure vaccination certificate creation and verification, and makes minimal use of CPU and memory.

The Mobile Blockchain Decentralized Application (DAPPS): A case study of IPTM Blockchain Certificate Verification System [13] describes a Certificate Verification System using blockchain technology. The system requires three nodes running 24/7 and an old desktop computer to maintain a decentralized model. The system is cost-effective, with a monthly maintenance cost of only \$7.26. The smart contract and Android Mobile DApps are open-source scripts that can be duplicated and improved by other academics.

The Development and Evaluation of Blockchain-based Secure Application for Verification and Validation of Academic Certificates [14] proposes a simple program that only requires a few clicks to use. Depending on future technology development, the program could potentially connect to many P2P networks, such as IPFS, Ethereum, and other systems. Institutions can use the application to help with the deployment of certificates and the development of the project.

The Generating E-Certificate and Validation using Blockchain [15] study proposes a blockchain-based system that reduces the possibility of certificate forgery. The automatic certificate-granting process and the application process are both open and visible in the system. As a result, organizations or corporations can query the system for details about any certificate.

III. PROPOSED SYSTEM

Certificates are uploaded onto IPFS via an IPFS Gateway in the solution we're recommending. A distributed system called IPFS is used to store and access files, webpages, programs, and data. Instead of uploading certificates as a pdf with all the graphic information, we use JSON files. A hash that may be shared with anybody for certificate verification reasons is returned to the user once the JSON file has been submitted.

A. Steps involved in the proposed system

1. Adding information to the certificate: The certifying authority is allowed to provide information such as the Beneficiary Name, Certificate Description, Expiration Date, Institute/Authority Name, and Additional Notes. To add a new certificate to the IPFS, the certifying authority can include this information.
2. The output from the transaction will be a transaction hash, which the certifying authority will get when the certificate is posted to the IPFS. The recipient will receive this. Additionally, the beneficiary will provide this transaction hash to anyone requesting access to their credentials.

Ethereum is the digital money that we are utilizing for our project. We'll make use of the Goerli test network to evaluate the system.

We will use much less blockchain space because we are submitting a JSON file rather than a PDF with illustrations. Additionally, this will significantly reduce processing time. The user experience will be enhanced overall in terms of processing and reaction time by all of this.

While using a commercial and dedicated IPFS Gateway, reaction times will be in a fraction of a second, compared to all this speed improvement when using a free IPFS Gateway.

B. Accessing the IPFS

We are utilizing the pinata IPFS Gateway in our project. Using the Pinata SDK, we are connecting to the gateway. The references section contains a link to the related documentation. In addition, we are also sending queries to the Pinata APIs using the Axios NPM package. We can send GET and POST requests to the Pinata API using Axios.

C. Architecture Diagram

The architecture we'll use for this project is shown in detail in the diagram below. We will IPFS upload the JSON objects containing all the necessary certificate information. We then provide the user with a shareable link that may be used to check the document's legitimacy.

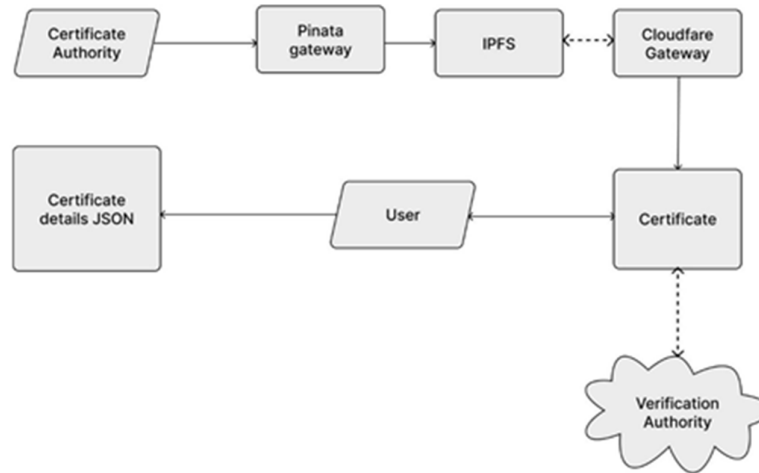


Figure 1. Architecture Diagram

IV. CONCLUSION

We have a secure online certificate issuance system in place for our project. This system employs a foolproof methodology that is error resilient. Since the address of the issuing authority will be plainly available on Etherscan and forged certificates may be easily detected, it is impossible to replicate or fabricate certificates.

FUTURE ENHANCEMENT

In the future, we will be able to encrypt the JSON files that are posted to IPFS. In this manner, we may strengthen the certification procedure's security measures. As a result, it will be more difficult to counterfeit or alter the certificates once they have been issued. Revocation of certificates by the certification authority could be included as another functionality. Additionally, we can include a choice allowing the certification authority to reinstate certificates that have been revoked.

REFERENCES

- [1] Andola, Nitish, et al. "Tamper-Proof Certificate Management System." 2019 *IEEE Conference on Information and Communication Technology*. IEEE, 2019.
- [2] Vidal, Fernando Richter, Feliz Gouveia, and Christophe Soares. "Revocation mechanisms for academic certificates stored on a blockchain." 2020 *15th Iberian Conference on Information Systems and Technologies (CISTI)*. IEEE, 2020.
- [3] Xie, Rui, et al. "Ethereum-blockchain-based technology of decentralized smart contract certificate system." *IEEE Internet of Things Magazine* 3.2 (2020): 44-50.
- [4] Ahubele, B. O., and O. E. Ndukwe. "A Verified Ethereum-Based Smart Contract Model to Detect Counterfeit Educational Certificate." *Journal, Advances in Mathematical & Computational Sciences* 9.2 (2021).
- [5] Lamkoti, Ravi Singh, et al. "Certificate Verification using Blockchain and Generation of Transcript." *Int. J. Eng. Res. Technol* 10.3 (2021).
- [6] Sarmah, Simanta Shekhar. "Application of blockchain in cloud computing." *International Journal of Innovative Technology and Exploring Engineering (IJITEE)* 8.12 (2019): 4698-4704.

- [7] Malsa, Nitima, et al. "Framework and Smart Contract for Blockchain Enabled Certificate Verification System Using Robotics." *Machine Learning for Robotics Applications*. Springer, Singapore, 2021. 125-138.
- [8] Rupa, Chiramdasu, et al. "Knowledge engineering–Based DApp using blockchain technology for protract medical certificates privacy." *IET Communications* 16.15 (2022): 1853-1864.
- [9] Bele, Roshani S., and Jayant P. Mehare. "A review on digital degree certificate using blockchain technology." *IJCRT* 9.2 (2021): 2320-2882.
- [10] Cheng, Jiin-Chiou, et al. "Blockchain and smart contract for digital certificate." 2018 *IEEE international conference on applied system invention (ICASI)*. IEEE, 2018.
- [11] Shanmuga Priya R, and Swetha N "Online Certificate Validation Using Blockchain" *International Journal of Advanced Networking and Applications - IJANA* (2019)
- [12] Mwrwan Abubakar, Pádraig McCarron, Zakwan Jaroucheh, Ahmed Al-Dubai and William J Buchanan "Blockchain-based Platform for Secure Sharing and Validation of Vaccination Certificates" *IEEE SINCONF 2021* (14th International Conference on Security of Information and Network) (2021)
- [13] Mohd Anuar Mat Isa, Muzaffar Hamzah and Daimler Benz Alebaba "Mobile Blockchain Decentralized Applications (DApps): A Case Study Of IPTM Blockchain Certificate Verification System" *Templat Penyediaan Manuskrip Karya Suntingan* (2021)
- [14] Elva Leka and Besnik Selimi, "Development and Evaluation of Blockchain based Secure Application for Verification and Validation of Academic Certificates" *Annals of Emerging Technologies in Computing (AETiC)* Vol. 5, No. 2, 2021
- [15] Rohan Hargude, Ghule Ashutosh, Abhijit Nawale, Pro.Sharad Adsure. "Generating E-Certificate and Validation using Blockchain" *International Journal of Creative Research Thoughts (IJCRT)* Vol. 9, Issue. 7, (2021)