



BLOCKIFICATE

E-Learning Platform Where Certificate is Powered by Blockchain

Author - Mr. Nikunj Panchal

Student,

Patkar Varde College, Mumbai, India

Abstract: Today's world is constantly emerging with new technologies and advancements. There are so many new things to learn about and for that nowadays, with the explosion of online learning platforms, many students are studying independently by purchasing courses online, following them, and gaining information, experience, and most importantly getting certified. However, some people frequently commit fraud by making a fake certificate for themselves in an effort to gain recognition. Implementing the idea of storing each student's certificate on blockchain in order to prevent these kinds of activities because blockchain is secure & transparent. As a result, we can make integrity stronger than ever before because some types of these wrong activities are still happening even after creating many securities & uniqueness in providing certificates. The certificate kept on this blockchain application system can be easily checked and verified by any institute or organization.

Index Terms: E-Learning, Certificate, Blockchain, IPFS, Peer-to-Peer, Smart Contract, Decentralization.

I. INTRODUCTION

A recent innovation in open networked secure computing without centralized authority is blockchain technology. A blockchain is a distributed database that logs an ever-evolving list of transaction records by arranging them into a hierarchical chain of blocks from the perspective of data management. The blockchain is constructed and maintained using a peer-to-peer overlay network, and it is secured utilizing crowd computing and intelligent, decentralized use of cryptography. There is an increasing concern about data security and surveillance as more people utilize the Internet. Furthermore, these systems demand outside assistance. These outside parties gather and manage the data, which could lead to security flaws. Blockchain technology has the potential to partially solve some of these problems. Blockchain is a peer-to-peer distributed technology that has a collection of data called Blocks that is always expanding. Each peer receives an exact duplicate of the data that is present on the Blockchain when data is transferred across peers in this manner.

The E-learning community has grown significantly, particularly during the COVID era. Online education degrees and courses are now available practically anywhere in the world. This action is still ongoing, which is fantastic in its own right. It's nice that some people were judged based on their actual skills and background. However, some of them have developed original strategies for deceiving institutions or organizations. Discovered that fake certificates are being created to be recognized for requirements that a person actually hadn't met. As a result, an unauthorized person is gaining access to positions where real people with knowledge and experience aren't being placed despite putting forth a lot of effort. The community of real strugglers will benefit much from this notion in its unique way by eliminating this unlawful practice. This project can be applied for security, authenticity, and transparency not only in this eLearning process but also in other similar sectors where a person's ability evaluation or a person's selection in some particular domain on some criteria. There isn't an existing project similar to this that has been found as of yet, but Coursera does offer a method for verifying their course certificate. However, since all the data is stored in a single, centralized database, anyone can tamper with it. In this project, we use blockchain to do away with this process because once data is stored in the blockchain, it can no longer be altered.

II. LITERATURE REVIEW

According to Rajalakshmi A, Lakshmy K V, Sindhu M, and Amritha P P, When kept on a central server, it may cause issues with efficiency. Consequently, a distributed system that is effective and secure is required. Blockchain is a new technology that aims to address these problems by building distributed environments with tamper-proof events of data. With content-addressability, peer-to-peer distributed file storage is how IPFS is intended to store hypermedia.[1]

According to Yongle Chen, Hui Li, Kejiao Li, and Jiyang Zhang, IPFS is a peer-to-peer version-controlled filesystem, It incorporates lessons learned from numerous prior successful systems. IPFS combines a self-certifying namespace, an incentive block exchange, and a distributed hash table. IPFS is a peer-to-peer hypermedia protocol designed to speed up, secure, and open up the internet. They want to create a better P2P file system built on IPFS and Blockchain-based on IPFS's qualities. Taking into account storage costs, dependability, availability, and other concerns for service providers. [2]

According to Muqaddas Naz, Fahad A. Al-zahrani, Rabiya Khalid, Nadeem Javaid, Ali Mustafa Qamar, Muhammad Khalil Afzal, and Muhammad Shafiq, Data sharing, is a crucial step in order to maximize the information gained from previous efforts. Current data-sharing platforms rely on a trusted third party (TTP). Such systems lack trust, transparency, security, and immutability because of the presence of TTP. This article proposes an Interplanetary file system-based blockchain-based secure data-sharing platform to address these problems (IPFS).[3]

FileShare is a safe decentralized application framework for file and data provenance sharing, and it is introduced by Shreya Khatal, Jayant Rane, Dhiren Patel, Pearl Patel, and Yann Busnel. It solves the integrity and ownership problems with the current data management and file-sharing systems. In the suggested framework, user registration and provenance are handled by a Decentralized Application (dApp) built on top of Ethereum. To control, administer, and provide visibility into the shared content's history from its inception to the most recent version, Ethereum smart contracts are deployed. It avoids the drawbacks of centralized storage systems by using the distributed file system IPFS as its data storage layer. The suggested framework makes use of a built-in editor to browse and edit files.[4]

According to Huawei Huang, Jianru Lin, Baichuan Zhenh, Zibin Zheng, and Jing Bian, Building globally distributed file systems (DFS) has drawn a lot of attention, Distributed file systems that use traditional peer-to-peer (P2P) technology inherently have flaws such instability, lack of auditing, and lack of incentive systems. Thus, a new generation of distributed file systems, represented by Inter-Planetary File System (IPFS) and Swarms, which connect with blockchain technologies, is suggested.[5]

III. METHODOLOGY

A. Register and Login

The Student will first Register and Login by Themselves for Conducting Different

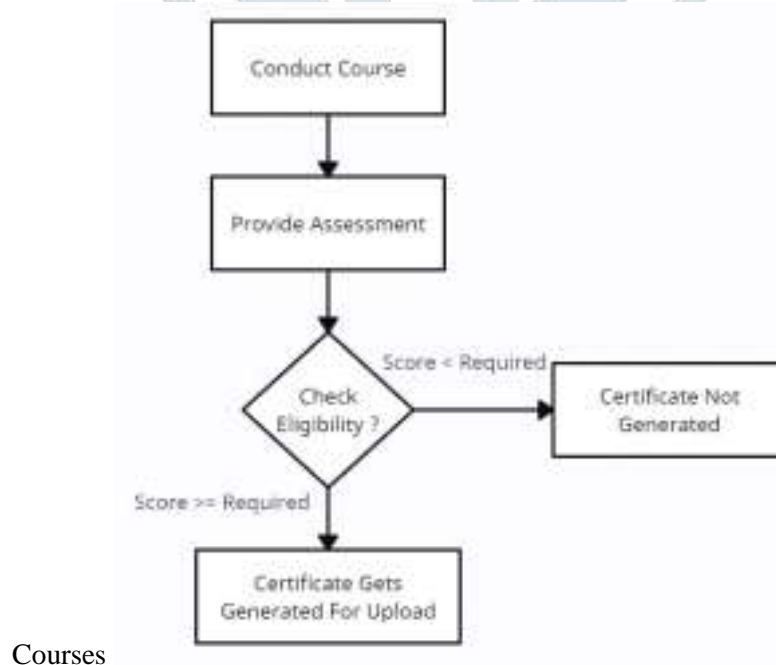


Fig.3.1 Certificate Generation

B. Uploading Certificate & Maintaining Hash for Student

After getting the required score certificate gets ready for uploading in IPFS



Fig. 3.2 Uploading and Maintaining Hash

C. Checking if Certificate is Present

When a student requests the certificate, the software first checks whether the hash is present in the blockchain or not. If it is not present then it shows the error "No Certificate is Uploaded". If it is present then the student gets the certificate.

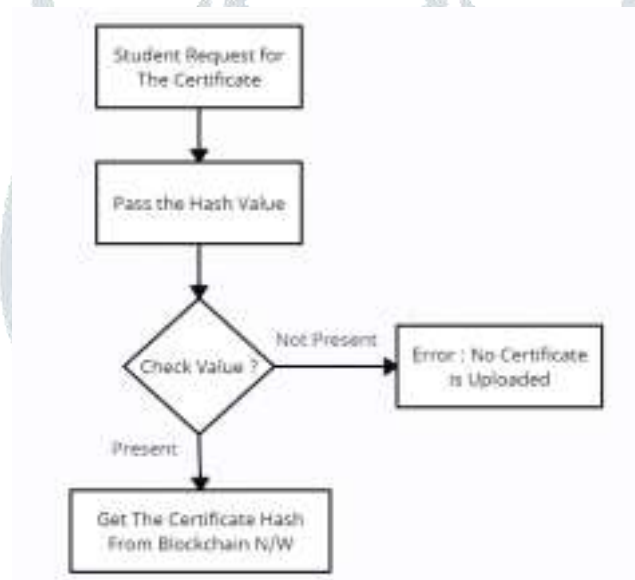


Fig. 3.3 Check for Certificate

D. Downloading Certificate

Student can see their certificate by passing the hash value in the IPFS URL link

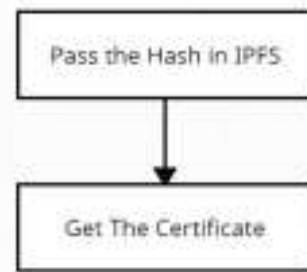


Fig. 3.4 Getting Certificate

E. System Architecture

The figure below shows the proposed architecture of the Blockificate website. The student creates an account and logs in, conducts course, and provides assessment based on that course. After that if the student scores the required points, then a certificate will get generated and uploaded in IPFS which stands for Interplanetary File System which is known as DFS (Decentralized File System), IPFS returns the hash value for the certificate which is also the address location of the certificate file, which hash later on uploaded to the Blockchain Network for Security, Immutability & Transparency. Student can retrieve their file by passing this hash value into the IPFS URL link.

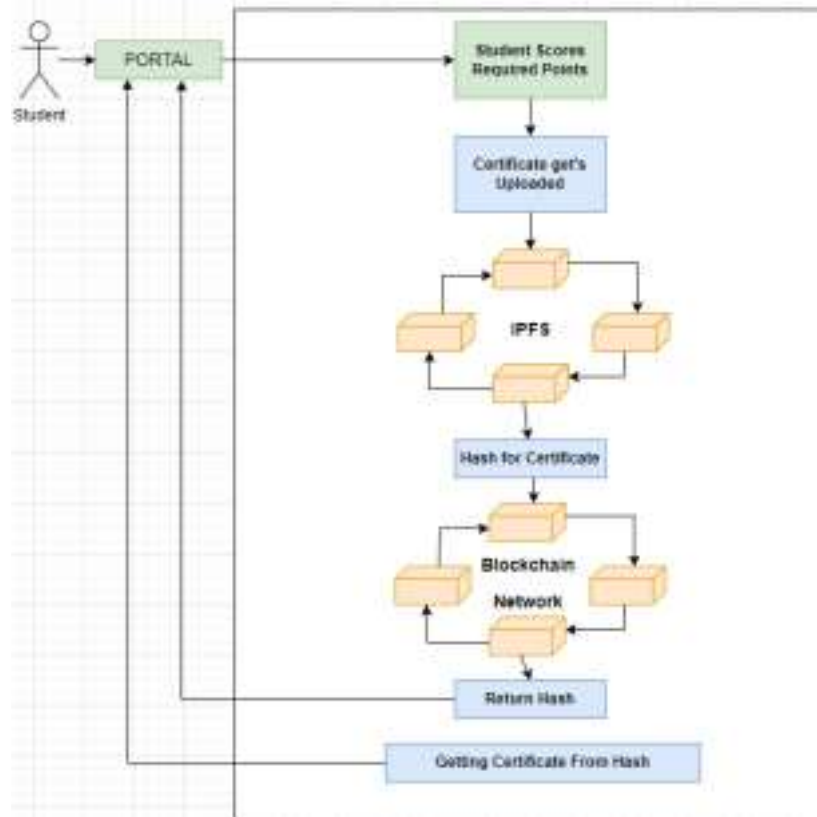


Fig. 3.5 System Architecture

IV. RESULT AND DISCUSSION

The project's conclusion is that dishonest behaviour needs to be reduced, and sincere individuals need to be given preference in every field. This project is a small attempt to accomplish that goal & tried to create a completely decentralized system without any centralized authority that might lead to data fraud.

Here is the difference between the existing system and the proposed system that will help you to understand the need for this approach.

Table 4.1 Comparison of Existing System and Proposed System

Existing System	Proposed System
Data breaches and file manipulation can occur at the server end in centralized systems because there is a single point of control for all data.	In contrast, blockchain and IPFS are decentralized systems with no central authority having control over data or the ability to tamper with data.
A centralized server for data storage may not be reliable from a computational and financial standpoint.	In Blockificate certificate data is stored in many peers and accessibility to these peers is fast as compared to any centralized server, HASH which is returned from IPFS is the only thing which is stored in the blockchain network which costs very less amount.

<p>Udemy, Coursera, NPTEL, Swayam, etc. are some examples of E-Learning System which provides E Certificate but here they have authority over a centralized server where these certificates are stored.</p>	<p>Whereas Blockificate is doing the same thing till certificate generation but after that, it will store the certificate on IPFS and store the reference hash value into the Blockchain network which is not controlled by any central authority.</p>
---	--

V. CONCLUSION

Blockificate presents a novel approach to address the challenges of decentralized file storage and sharing using the IPFS and blockchain technologies. The implementation of the project utilized smart contracts, IPFS storage, and a user-friendly web application built with React.js. It's main focus is on ensuring data security, accessibility, and privacy for the users. It's success can be attributed to the efficient and reliable integration of IPFS and blockchain technologies, enabling secure, decentralized file storage and sharing. And so, BLOCKIFICATE provides a strong foundation for future work in the field of decentralized data storage and sharing and can thus prove to be of utmost help for data frauds and fake course or certificate claims.

VI. REFERENCES

- [1] Rajalakshmi A, Lakshmy K V, Sindhu M and Amritha P P, A Blockchain and IPFS based framework for secure Research record keeping <https://acadpubl.eu/hub/2018-119-15/4/751.pdf>
- [2] Yongle Chen, Hui Li, Kejiao Li and Jiyang Zhang, [An improved P2P file system scheme based on IPFS and Blockchain | IEEE Conference Publication | IEEE Xplore](#)
- [3] Muqaddas Naz, Fahad A. Al-zahrani, Rabiya Khalid, Nadeem Javaid1, Ali Mustafa Qamar, Muhammad Khalil Afzal and Muhammad Shafiq, A Secure Data Sharing Platform Using Blockchain and Interplanetary File System https://res.mdpi.com/d_attachment/sustainability/sustainability-11-07054/article_deploy/sustainability-11-07054.pdf
- [4] Shreya Khatal, Jayant Rane, Dhiren Patel, Pearl Patel, Yann Busnel, [FileShare: A Blockchain and IPFS framework for Secure File Sharing and Data Provenance \(hal.science\)](#)
- [5] Huawei Huang, Jianru Lin, Baichuan Zheng, Zibin Zheng, And Jing Bian, [When Blockchain Meets Distributed File Systems: An Overview, Challenges, and Open Issues \(ieee.org\)](#)
- [6] IPFS, [IPFS Powers the Distributed Web](#)
- [7] Ethereum, [Home | ethereum.org](#)